Secret Key Generation Via Localization and Mobility in Wireless Networks

Onur Gungor, Fangzhou Chen, C. Emre Koksal

Department of Electrical and Computer Engineering
The Ohio State University, Columbus, 43210

***Abstract*—We consider secret key generation from relative localization information of a pair of nodes in a mobile wireless network in the presence of a mobile eavesdropper. Our proposed algorithm consists of the following phases: in the first phase, legitimate node pair opportunistically exchanges beacon signals to establish localization information based on noisy observations of these beacons. Then, the nodes generate secret key bits via a public discussion and privacy amplification. Our problem can be categorized under the source models of information theoretic secrecy, where the distance between the legitimate nodes acts as the observed common randomness. We also characterize theoretically achievable secret key bit rate in terms of the observation noise variance at the legitimate nodes and the eavesdropper, and show that the performance of our algorithm is comparable to the theoretical bounds. This work provides a framework that combines information theoretic secrecy and wireless localization, and proves that the localization information provides a significant additional resource for secret key generation in mobile wireless networks.**

I. Introduction

We consider the generation of a common key in a pair of nodes, which move in $\mathbb{R}^2$ (continuous space) according to a discrete time stochastic mobility model. We exploit the reciprocity of the distance between a given pair of locations, view the distance between the legitimate nodes as a common randomness shared by these nodes and utilize it to generate secret key bits using the ideas from source models of secrecy.

To that end, we propose a key generation algorithm, in which the legitimate nodes use a four-stage key generation process: (1) In the first stage, they opportunistically exchange wireless beacons to obtain information regarding the sequence of distances between them over many time slots as they move in the area. The beacon signal may contain explicit information such as a time stamp, or the receiving node can extract other means of localization information by analyzing the angle of arrival, the received signal strength, etc. (2) In the second stage, the nodes perform localization based on the observations of distances, and the statistics of the mobility model, and obtain estimates of their relative locations with respect to each other. (3) In the third stage, the nodes communicate over the public channel to agree on an initial key based on their relative location estimates. Meanwhile, the eavesdropper also obtains some information correlated with the generated key. (4) In the final stage, the legitimate nodes perform privacy amplification on the initial key to obtain the final key. The generated final key bits satisfy the following three quality measures i) reliability, ii) secrecy, and iii) randomness. For reliability, we show that the probability of mismatch between the keys generated by the legitimate nodes decays to 0 with increasing block length. In our attacker model, we consider a single passive eavesdropper, that is not allowed to transmit any wireless signal, overhears the exchanged beacons in the first phase, and the public discussion in the third phase, and tries to deduce the generated key based solely on these observations. For secrecy, we consider Wyner's notion, i.e., the rate at which mutual information on the key leaks to the eavesdropper should be arbitrarily low. For randomness, the generated key bits have to be perfectly compressed, i.e., the entropy should be equal to the number of bits it contains.

We also focus on the theoretical limits in key rate performance. Using a source model of secrecy, we characterize the achievable secret key bit rate in terms of the observation noise variance at the legitimate nodes and the eavesdropper under two different cases of global location information (GLI). We first consider no GLI, in which the nodes do not observe their global locations directly. Then we consider perfect GLI, in which nodes have perfect observation of their global locations, through a GPS device, for example. We show that, under both cases, localization information provides a significant additional resource for secret key generation. We also study the beacon power asymptotics of the system. We show a phase-transition phenomenon for the key rate, as

The authors are with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH, 43210. This work was in part presented in the workshop on Physical Layer Security, Globecom 2011. This draft is an extended version of the manuscript submitted to JSAC, Special Issue on Signal Processing Techniques for Wireless Physical Layer Security.

it varies relative to the eavesdropper's angle observation. In particular, we prove that the secret key rate grows unboundedly with the beacon power, if the eavesdropper does not obtain the angle of arrival observations of the beacon signals. Otherwise, even with a highly noisy angle of arrival observation, it is not possible to increase the secret key rate beyond a certain limit by increasing the beacon power.

Assuming the beacon observations are readily available, we implement our key generation algorithm and compare the achieved key rates with the established theoretical bounds as a function of beacon power. We show that our algorithm achieves key rate close to the theoretical lower bound at a bit mismatch probability less than 0.001 at the legitimate nodes and an information leakage rate of less than 0.001 bits/sample to the eavesdropper. For the measure of randomness, we use the NIST test suite [25]. We show that the generated key passes all the randomness tests in the NIST test suite.

The opportunistic nature of our algorithm comes from the fact that the beacons are exchanged only when they predict a geographic advantage over the eavesdropper, based on their past observations. We show that non-zero key rates can be guaranteed by this opportunistic scheme, even when the eavesdropper obtains better localization information *on average*. We also study the eavesdropper's mobility strategies to reduce the secret key rate. We specifically consider the strategy where the eavesdropper moves to the middle of its location estimates of the legitimate nodes. We show through simulations that with this strategy, the eavesdropper can significantly reduce the secret key rate compared to the case where it follows a random mobility pattern.

II. Related Work

Source model of secrecy studies generation of secret key bits from common randomness observed by legitimate nodes. In his seminal paper [1], Maurer showed that, if two nodes observe correlated randomness, then they can agree on a secret key through public discussion. He provided upper and lower bounds on the achievable secret key rates, considering that the nodes have unlimited access to a public channel, accessible by the eavesdropper. Although the upper and lower bounds have been improved later [2], [3], the secret key capacity of the source model in general is still an open problem. Despite this fact, the source model has been utilized in several different settings [4]–[6].

There is a vast amount of literature on localization in wireless networks (see, e.g., [7]–[9], and the references therein). There has been some focus on secure localization and position-based cryptography [10]–[13], however, these works either consider key generation in terms of other forms of secrecy (i.e., computational secrecy), or fall short of covering a complete information theoretic analysis. Also a similar line of work in wireless network secrecy considers channel identification [14] for secret key generation in Ultrawideband Channels. Based on the channel reciprocity assumption, nodes at both ends experience the same channel, corrupted by independent noise. Therefore, nodes can use their channel magnitude and phase response observations to generate secret key bits from public discussion. In [21], it is shown that key generation can also be achieved with on-the-shelf devices, where they show achievability of key rates above 1 bit/s under 802.11 development platform. In [22], effectiveness of key generation is questioned, focusing on a scenario in which the legitimate nodes generate secret key bits based on the received signal strength (RSS). The authors show that the eavesdropper, knowing the location of the legitimate nodes, can force the legitimate nodes to generate deterministic key bits by periodically blocking and un-blocking their line-of-sight. This paper shows the relationship between localization and channel identification. [23] focuses on overcoming this type of attack by considering key generation based on channel impulse response based on node locations. Keys are generated from a large amount of observations, and non-zero secret key bits are achieved with the assumption that the eavesdropper cannot always be in a geographical advantage. In [24], the authors improve upon the previous works by using more sophisticated signal processing methods to achieve secret key rates as high as 22 bits/s.

As pointed out in [22], localization is fundamentally related to key generation based on channel identification. The fact that the eavesdropper's channel observation is independent of the legitimate nodes' channel observations may not be correct when the eavesdropper knows the locations of the legitimate nodes. Our approach of key generation based on locations, on the other hand, is *fundamentally secure* against a passive eavesdropper, as we can explicitly calculate the equivocation rate.

The rest of this paper is organized as follows. In Section III, we give the system model, and in Section IV, we provide our key generation algorithm. In Section V, we study the theoretical performance limits of key generation from localization. In Section VI, we provide numerical evaluation of the theoretical limits given in this paper, and compare the performance of our key generation algorithm with these limits. We conclude in Section VII. To enhance the flow of the paper, several proofs and derivations are collected in Appendix.

A word about notation: We use $[x]^+ = \max(0, x)$ and $\|.\|$ denotes the L2-norm.A brief list of variables used in the paper can be found in Table I.

TABLE I: List of variables

var.	Description
d_{ij}	distance between nodes i and j
l_j	2-D location of node j
ϕ_{ij}	angle between nodes i and j
$\hat{d}_j, \hat{\phi}_j$	observation of nodes $j \in \{1,2\}$ of d_{12} and ϕ_j
$\hat{d}_{je}$	observation of node e of d_{je} and ϕ_{je}
o_j	complete observations of node j based on available GLI
γ	Noise variance coefficient due to path loss
ρ	Noise variance coefficient due to node capability
s	location triple $[l_1, l_2, l_e]$
s^Δ	quantized version of location triple, $[l_1^\Delta, l_2^\Delta, l_e^\Delta]$
Δ	quantization resolution
ψ	quantization function
$\tilde{s}_j^\Delta$	node j's estimate of s^Δ based on all of its information
$\tilde{d}_j^\Delta$	quantized distance estimates extracted from $\tilde{s}_j^\Delta$
κ	binary conversion function
v_j	obtained binary key at node j before public discussion
u_j	obtained binary key at node j after public discussion
k_j	final key at node j after privacy amplification

III. System Model

A. Mobility Model

We consider a simple network consisting of two mobile legitimate nodes, called user 1 and 2, and a possibly mobile eavesdropper e. We divide time into n discrete slots, where slot $i \in \{1, \cdots, n\}$ covers the time interval $[iI,\ (i+1)I)$. Let $l_j[i] \in \mathbb{R}^2$ be the random variable that denotes the coordinates of the location of node $j \in \{1,2,e\}$ in slot i. We use the boldface notation $\mathbf{l}_j = \{l_j[i]\}_{i=1}^n$, to denote the n-tuple location vectors for $j \in \{1,2,e\}$. The distance between nodes 1 and 2 in slot i is $d_{12}[i] = \|l_1[i] - l_2[i]\|$. Similarly, $d_{1e}[i]$ and $d_{2e}[i]$ denote the sequence of distances between nodes $(1,e)$ and nodes $(2,e)$ respectively. We use the boldface notation $\mathbf{d}_{12}$, $\mathbf{d}_{1e}$, $\mathbf{d}_{2e}$ for the n-tuple distance vectors. Furthermore, let $\phi_e[i]$ be the angle of the triangle at node e at slot i, and $\boldsymbol{\phi}_e = \{\phi_e[i]\}_{i=1}^n$. In any slot, the nodes form a triangle in $\mathbb{R}^2$, as depicted in Figure 1. We assume that the location vectors $\mathbf{l}_1, \mathbf{l}_2, \mathbf{l}_e$ form an

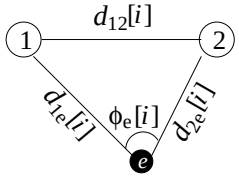

Fig. 1: Legitimate nodes and the eavesdropper form a triangle.

ergodic Markov process, and their joint probability density function $f(\mathbf{l}_1, \mathbf{l}_2, \mathbf{l}_e)$ is well defined[1]. We assume that the distances $d_{12}[i],\ d_{1e}[i],\ d_{2e}[i]$ take values in the interval $[d_{\min}\ d_{\max}]$, since the nodes cannot be closer to each other than $d_{\min}$ due to physical restrictions, and they cannot be further than $d_{\max}$ away to each other due to their limited communication range.

B. Beacon Exchange

At the beginning of each time slot, there is a beacon exchange period, in which the pair of nodes exchange beacon signals in order to obtain information about their relative position with respect to each other. There are various methods to establish the localization information from the beacon signals, e.g., by using the propagation delay (time of arrival) of electromagnetic signals [7]. In this paper, we will not treat these methods separately. We will simply assume that, during each beacon exchange period i, when node 1 transmits a beacon, nodes 2 and e obtain a noisy observation of $d_{12}[i]$ and $d_{1e}[i]$ respectively. Let these observation be $\hat{d}_2[i]$ and $\hat{d}_{1e}[i]$. Similarly, when node 2 follows up with a beacon, nodes 1 and e observe $\hat{d}_1[i]$ and $\hat{d}_{2e}[i]$, respectively. With the observations of both the beacons, the eavesdropper also obtains a noisy observation, $\hat{\phi}_e[i]$, of the angle between the legitimate nodes. We emphasize that, the observations in each slot are obtained solely from the beacons exchanged during that particular slot. The nodes' final estimates of the distances depend also on the observations during other slots, due to predictable mobility patterns.

Note that the availability of global location information (GLI) at the legitimate nodes would also enable them to observe the angle between with respect to some coordinate plane (e.g., $\phi_{12}[i]$ as shown in Figure 2). To that end, we consider the following two extreme cases:
1) no GLI: the nodes do not have any knowledge of their global location, and
2) perfect GLI: each node has perfect knowledge of its global location.
Let $o_j[i]$ denote the set of observations of node $j \in \{1,2,e\}$ during slot i. The observations $o_j[i]$ for each case is provided in Table II. Note that with perfect GLI, all nodes have a sense of orientation with respect to some coordinate plane as shown in Figure 2. In this case, nodes 1, 2 obtain noisy observations $\hat{\boldsymbol{\phi}}_1,\ \hat{\boldsymbol{\phi}}_2$ of the angle $\boldsymbol{\phi}_{12}$. Similarly, node e obtains noisy observation $\hat{\boldsymbol{\phi}}_{1e},\ \hat{\boldsymbol{\phi}}_{2e}$ of the angles $\boldsymbol{\phi}_{1e}, \boldsymbol{\phi}_{2e}$. To develop our op-

TABLE II: Nodes' Observations

	No GLI	Perfect GLI
$o_1[i]$	$[\hat{d}_1[i]]$	$[\hat{d}_1[i], \hat{\phi}_1[i], l_1[i]]$
$o_2[i]$	$[\hat{d}_2[i]]$	$[\hat{d}_2[i], \hat{\phi}_2[i], l_2[i]]$
$o_e[i]$	$[\hat{d}_{1e}[i], \hat{d}_{2e}[i], \hat{\phi}_e[i]]$	$[\hat{d}_{1e}[i], \hat{d}_{2e}[i], \hat{\phi}_{1e}[i], \hat{\phi}_{2e}[i], l_e[i]]$

[1]Note that, these assumptions are not vital for our key generation algorithm, rather are present for the ease of calculation of achievable key rates

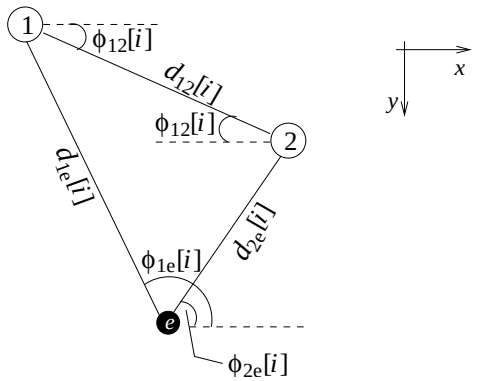

Fig. 2: With GLI, the nodes obtain noisy observations of the relative orientation of each other with respect to the x-axis.

portunistic beacon exchange algorithm and analyze the key rate performance [2], we specifically focus on the case where the nodes obtain distance and angle observations corrupted with additive Gaussian noise, i.e.,

$$\hat{d}_j[i] = d_{12}[i] + w_j[i],\ j \in \{1,2\} \quad (1)$$
$$\hat{d}_{je}[i] = d_{je}[i] + w_{je}[i],\ j \in \{1,2\} \quad (2)$$
$$\hat{\phi}_e[i] = \phi_e[i] + w_{\phi_e}[i], \quad (3)$$

where

$$w_j[i] \sim \mathcal{N}\left(0, \frac{\gamma(d_{12}[i])\rho_j}{P}\right)$$
$$w_{je}[i] \sim \mathcal{N}\left(0, \frac{\gamma(d_{je}[i])\rho_e}{P}\right)$$
$$w_{\phi}[i] \sim \mathcal{N}\left(0, \frac{\gamma_\phi(d_{1e}[i], d_{2e}[i])\rho_e}{P}\right).$$

Here, P is the beacon power, and γ is an increasing function of the distance, and it solely depends on the characteristics of the wireless medium such as the path loss exponent. Similarly, $\gamma_\phi(d_{1e}[i], d_{2e}[i])$ determines the angle observation error, and is an increasing function of both distances $d_{1e}[i]$ and $d_{2e}[i]$. The parameter ρ_j, depends on the capability of the nodes, and is smaller for nodes with higher capability, e.g., with MIMO, or higher antenna gain. Similarly, the angle observations in the perfect GLI case follow Gaussian distribution

$$\hat{\phi}_j[i] = \phi_j[i] + w_{\phi_j}[i],\ j \in \{1,2\} \quad (4)$$
$$\hat{\phi}_{je}[i] = \phi_{je}[i] + w_{\phi_{je}}[i],\ j \in \{1,2\} \quad (5)$$
$$(6)$$

[2]Part of this model has been used in the literature to characterize the distance observation noise when time-of-arrival estimation technique is used [7], [18]. In fact, the distance observation noise cannot be perfectly Gaussian. However, under the assumption $\mathbb{E}[\gamma(\cdot)] \ll d[\cdot]$, the Gaussian assumption is reasonable. Furthermore, there there may be a bias on these observations due to small scale fading [18]. The effect of biased observations are studied in Appendix C

where

$$w_{\phi_j}[i] \sim \mathcal{N}\left(0, \frac{\gamma_\phi(d_{12}[i])\rho_j}{P}\right)$$
$$w_{\phi_{je}}[i] \sim \mathcal{N}\left(0, \frac{\gamma_\phi(d_{je}[i])\rho_e}{P}\right).$$

For perfect GLI, the angle information is obtained according to a fixed coordinate plane, hence the function γ_ϕ has single argument. Clearly, the achievable key rates depend highly on the functions γ, γ_ϕ and ρ. We will show that, our algorithm achieves non-zero secret key rates even when the eavesdropper is more capable, i.e., $\rho_e < \rho_j$, for $j \in \{1,2\}$. In Section VI, we evaluate the key rate performance of our algorithm for particular choices of γ, γ_ϕ and ρ, and compare with the theoretical bounds provided in Section V-A.

We emphasize that, our key generation algorithm works in the general case, without the above assumptions on the distance and angle observations. In fact, we provide the theoretical key rate performance without these assumptions on Section V-A. Also note that in some cases, the nodes cannot obtain any useful angle information. For instance, when each node is equipped with a single omnidirectional antenna, no angle observation may be possible. Also in the indoor setting without the line of sight, due to multipath reflections, it may be unlikely that the strongest signal component is observed directly from the transmitting station, but from a reflection instead. Thus, the angle observation may contain only minimal information regarding the direction of the transmitter, making the angle information highly noisy for the eavesdropper. In our analysis of such cases, we use $I(\hat{\boldsymbol{\phi}}_j; \boldsymbol{\phi}_j) = 0$ for legitimate nodes $j \in \{1,2\}$ in perfect GLI, $I(\hat{\boldsymbol{\phi}}_{je}; \boldsymbol{\phi}_{je}) = 0$ for the eavesdropper in perfect GLI, and $I(\hat{\boldsymbol{\phi}}_e; \boldsymbol{\phi}_e) = 0$ for the eavesdropper in no GLI.

C. Attacker Model

We assume that there exists a passive eavesdropper e, which does not transmit any beacons. However, we assume that e can strategically change its location to obtain a geographical advantage against the legitimate nodes. Overall, we consider two strategies:

Random Mobility: Eavesdropper moves randomly, without a regard to the location of the legitimate nodes. We will assume that eavesdropper adopts random mobility unless otherwise stated.

Mobile Man in the Middle: Node e *controls* its mobility, such that it can move accordingly to obtain a geographic advantage compared to legitimate nodes. Since the observation noise variances are monotonically increasing functions of the distance, we can see that it would be to the eavesdropper's advantage to stay in

between the legitimate nodes. Since the eavesdropper has an estimate of the current locations of the nodes, a reasonable strategy for it is to move to the mid-point of the most up to date estimates of the locations of the legitimate nodes. Thus, in slot i, the eavesdropper moves to location

$$\frac{\tilde{l}_{1,e}[i-1]+\tilde{l}_{2,e}[i-1]}{2}, \tag{7}$$

at the beginning of each slot i, where for $j \in \{1,2\}$,

$$\tilde{l}_{j,e}[i-1] = \max_{l} \mathbb{P}(l_j[i]|o_e[1],\ldots,o_e[i-1])$$

is the estimate of the location $l_j[i-1]$ given the eavesdropper's observations until the $i-1$'th slot.

D. Notion of security

We consider the typical definition of source model of information theoretic secrecy under a passive eavesdropper: We assume that there exists an authenticated error-free public channel, using which the legitimate nodes can communicate to agree on secret keys, based on the observations of the distances and angles ($\mathbf{o}_1$ and $\mathbf{o}_2$) obtained during beacon exchange. This process is commonly referred to as public discussion [1]. A public discussion algorithm is a T step message exchange protocol, where at any step $t \in \{1,\cdots,T\}$, node 1 sends message $C_1[t]$, and node 2 replies back with message $C_2[t]$ such that, for $t > 1$,

$$H\big(C_1[t]|\mathbf{o}_1, \{C_1[i]\}_{i=1}^{t-1}, \{C_2[i]\}_{i=1}^{t-1}\big) = 0, \text{ odd } i \tag{8}$$
$$H\big(C_2[t]|\mathbf{o}_2, \{C_1[i]\}_{i=1}^{t}, \{C_2[i]\}_{i=1}^{t-1}\big) = 0, \text{ even } i. \tag{9}$$

At the end of the T step protocol, node 1 obtains $\mathbf{k}_1$, and node 2 obtains $\mathbf{k}_2$ as the secret key, where

$$H\left(\mathbf{k}_j|\mathbf{o}_j, \{C_1[t], C_2[t]\}_{t=1}^{T}\right) = 0, \ j \in \{1,2\}. \tag{10}$$

Definition 1: We say that *perfectly reliable* key bits are generated (with respect to the described attacker model) at rate R, if, for all $\epsilon > 0$ and $\delta > 0$, there exists some $n,\ T > 0$ such that (8), (9) and (10) are satisfied, and

$$H(\mathbf{k}_j)/n = R, \ j \in \{1,2\}$$
$$\mathbb{P}(\mathbf{k}_1 \neq \mathbf{k}_2) \leq \epsilon$$
$$I(\mathbf{k}_j; \mathbf{o}_e, \{C_1[t], C_2[t]\}_{t=1}^{T})/n \leq \delta, \ j \in \{1,2\}. \tag{11}$$

To achieve perfect reliability, schemes proposed in the source model of secrecy typically use a random coding structure, where the messages $\{C_1[t], C_2[t]\}_{t=1}^{T}$ are generated by using a binning strategy [1]- [6]. In Section V, we will make use of these existing results to provide computable theoretical bounds on the achievable key rates. For most channel models, perfect reliability can only be achieved asymptotically, as the block size $n \to \infty$, and keys generated over any finite block size $n < \infty$ violates the conditions of perfect reliability. To that end, to evaluate the reliability of the generated key bits over finite blocks, we introduce a weaker notion of security. Before we provide that definition, let us define the bit mismatch rate at the legitimate nodes as

$$\text{BMR}_j = \frac{\sum_{i=1}^{nR} \mathbf{1}(k_1[i] \neq k_2[i])}{nR}$$

for $j \in \{1,2\}$, where $\mathbf{1}(\cdot)$ is the indicator function, which is equal to 1 when its argument is correct, and 0 otherwise.

Definition 2: We say that (ϵ,δ)-reliable key bits are generated at rate R, if

$$H(\mathbf{k}_j)/n = R, \ j \in \{1,2\}$$
$$\text{BMR}_j \leq \epsilon$$
$$I(\mathbf{k}_j; \mathbf{o}_e, \{C_1[t], C_2[t]\}_{t=1}^{T})/n \leq \delta, \ j \in \{1,2\}.$$

When evaluating our key generation algorithm, we provide the associated (ϵ,δ) pair at a given rate R.

IV. Key Generation Algorithm

Our proposed algorithm allow the legitimate nodes to generate secret key bits from their mobility patterns after following phases: *quantization*, *opportunistic beacon exchange*, *location estimation*, *public discussion* and *privacy amplification*. In this section, we briefly explain each part, and then provide the complete scheme in Algorithm 1.

A. Quantization

Prior to the first stage, the nodes quantize the state space $\mathbf{s} = [\mathbf{l}_1, \mathbf{l}_2, \mathbf{l}_e]$. Quantization is required for the nodes to efficiently calculate the location estimates and store them in their buffers for use in the subsequent public discussion phase. Let $\psi(\cdot)$ be a predetermined quantization function. Then, the legitimate nodes $j \in \{1,2\}$ can obtain quantized version of the state space as $\mathbf{s}^{\Delta} = [\mathbf{l}_1^{\Delta}, \mathbf{l}_2^{\Delta}, \mathbf{l}_e^{\Delta}]$, where $l_j^{\Delta}[i] = \psi(l_j[i], \Delta)$, and we define $|\Delta| \triangleq \max_x |x - \psi(x)|$ as the resolution of quantization. In our algorithm, we consider the uniform quantization method, where

$$\psi(x) = \arg\min \|k - x\|$$
$$\text{subject to: } k = \frac{u\Delta}{\sqrt{2}}, \ u \in \mathbb{Z}^2.$$

Similarly, we assume that the eavesdropper quantizer be represented with parameter Δ'.

B. Opportunistic Beacon Exchange

In this phase, the legitimate nodes exchange beacons to develop the common randomness which serves as the basis for key generation in the following steps. Beacons are exchanged over n subsequent slots to form the observation vectors $\mathbf{o}_1$ and $\mathbf{o}_2$ as outlined in Table II. Node e, on the other hand, overhears the beacons and obtains the observations $\mathbf{o}_e$. Note that at any slot i, $o_1[i]$, $o_2[i]$, and $o_e[i]$, are independent of each other given $s[i]$. Therefore, when $o_1[i]$ and $o_2[i]$ are both stochastically degraded versions of $o_e[i]$, i.e., there exists a density function $\tilde{f}$ such that the condition

$$f(o_j[i]|s[i]) = \int_{x=o_e[i]} f(x|s[i])\tilde{f}(o_j[i]|x)\mathrm{d}x \qquad (12)$$

holds for $j \in \{1,2\}$, transmission at slot i benefits the eavesdropper *more* than it benefits the legitimate nodes. This is due to the fact that, since node locations are not independent across time, the eavesdropper can use the advantage obtained at slot i to obtain better estimates at slot $i+1$. Therefore, skipping beacon transmission at slots when condition (12) occurs will yield *higher* key rates compared to the case where a beacon is exchanged in every slot.

In our opportunistic beacon exchange scheme, provided in Algorithm 2, the decision of beacon transmission in a slot is made by the the legitimate node that is more capable, i.e., the one with lower ρ_j. This node is defined to be the *master node*, and is chosen prior to the opportunistic beacon exchange phase. Let

$$A[i] = \frac{\big(d_{1e}[i] - d_{2e}[i]\cos(\phi_e[i])\big)^2\gamma(d_{1e}[i])}{d_{12}[i]^2} + \frac{\big(d_{2e}[i] - d_{1e}[i]\cos(\phi_e[i])\big)^2\gamma(d_{2e}[i])}{d_{12}[i]^2}$$

$$B[i] = \frac{(d_{1e}[i]d_{2e}[i]\sin(\phi_e[i]))^2\gamma_\phi(d_{1e}[i], d_{2e}[i])}{d_{12}[i]^2}.$$

Let $\rho_{\max} = \max(\rho_1, \rho_2)$. The master node decides to transmit a beacon at slot i either when the condition

$$\mathbb{P}\left(\gamma(d_{12}[i])\rho_{\max} > (A[i]+B[i])\rho_e | \{o_k[l]\}_{l=1}^{i-1}\right) < \tau \qquad (13)$$

holds for some predetermined threshold τ, or when no beacons have been transmitted in the previous c slots, chosen appropriately in order to avoid long droughts leading to the possibility for the nodes to get out of each other's range. The condition (13) is chosen such that the condition (12) holds. The derivation is provided in Appendix A. If the other legitimate node receives a beacon during slot i, it replies back with a beacon, otherwise it remains silent. At the end of slot i, the nodes update their observations, such that if no beacons have been transmitted, then $o_j[i] = \emptyset$ for $j \in \{1,2,e\}$.

The probability in (13) can be efficiently approximated with linear complexity using Forward Algorithm as follows. Due to the Markov assumption on the mobility model, the states $s^\Delta[i-1] \to s^\Delta[i] \to s^\Delta[i+1]$ form a Markov chain. Also, since the observations $o_j[i]$ are Gaussian, with a variance depending solely on the current state $s^\Delta[i]$, $o_j[i]$ is independent of $\{s^\Delta[k]\}_{k\neq i}$ given $s[i]$. Therefore, $s^\Delta[i]$'s and $o_j[i]$'s form a hidden Markov chain as depicted in Figure 3. Forward Algorithm follows from the simple observation that for any slot i,

$$f(o_j[1],\ldots,o_j[i],s^\Delta[i]) = \int f(o_j[1],\ldots,o_j[i-1], s^\Delta[i-1])\mathbb{P}(s^\Delta[i]|s^\Delta[i-1])f(o_j[i]|s^\Delta[i])\mathrm{d}s^\Delta[i-1]. \qquad (14)$$

The term $\mathbb{P}(s^\Delta[i]|s^\Delta[i-1])$ is called state transition probability, and is independent on current time slot i, since the mobility model is stationary. The term $f(o_j[i]|s^\Delta[i])$ is called emission density, which is Gaussian, as described by (1)-(3). Thus (14) gives us an iterative relationship to calculate $f(o_j[1],\ldots,o_j[i],s^\Delta[i])$ using $f(o_j[1],\ldots,o_j[i-1],s^\Delta[i-1])$. Iterating over (14) for n slots, we obtain $f(\mathbf{o}_j,\mathbf{s}^\Delta)$. Recall that $\mathbf{s}^\Delta = [\mathbf{l}_1^\Delta, \mathbf{l}_2^\Delta, \mathbf{l}_e^\Delta]$, the quantized states, contains quantized version of all the distance and angle information in (13), e.g., $(\mathbf{d}_{12}^\Delta, \mathbf{d}_{je}^\Delta, \boldsymbol{\phi}_e^\Delta)$. Hence, the probability in (13) can be efficiently calculated.

Note that if the mobility is i.i.d., then no advantage in terms of secret key rate can be obtained by using opportunistic beacon transmission. Still, power would be more efficiently utilized. In Section VI, we show that our algorithm achieves non-zero secret key rates for some cases that yield zero secrecy rates when a beacon is transmitted every time slot. We also compare our algorithm with the genie aided case, in which a genie knows the exact locations all the nodes in the field, and tells the nodes to skip beacon transmission at slot i when the condition

$$\gamma(d_{12}[i])\rho_{\max} > (A[i]+B[i])\rho_e$$

is satisfied. The genie aided case provides us an upper bound on the achievable key rate among algorithms that use this condition for beacon transmission decisions.

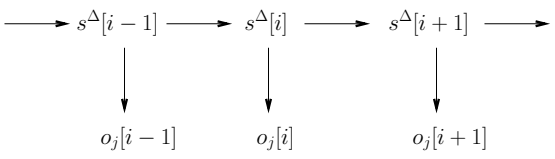

Fig. 3: The hidden Markov structure

C. Localization

In this phase, the legitimate nodes obtain the estimates $\tilde{\mathbf{s}}_1^\Delta$ and $\tilde{\mathbf{s}}_2^\Delta$ of the quantized location triple $\mathbf{s}^\Delta = [\mathbf{l}_1^\Delta, \mathbf{l}_2^\Delta, \mathbf{l}_e^\Delta]$ where

$$\tilde{\mathbf{s}}_j^\Delta = \arg\max_{\mathbf{s}_j^\Delta} \mathbb{P}(\mathbf{s}_j^\Delta | \mathbf{o}_j), \;\; j \in \{1,2\}. \tag{15}$$

Similar to the Forward Algorithm, the terms $\tilde{\mathbf{s}}_j^\Delta$ are obtained efficiently by using the Viterbi Algorithm in our scheme. Let

$$\chi_j(s^\Delta[i]) = \arg\max_{s^\Delta[1],\cdots,s^\Delta[i]} \mathbb{P}(s^\Delta[1],\cdots,s^\Delta[i] | o_j^\Delta[1],\cdots,o_j^\Delta[i])$$

denote the most likely sequence of node j based on its observations up to slot i. Then, Viterbi algorithm follows from the following relation for any i,

$$\begin{aligned} f(\chi_j(s^\Delta[i]), o_j^\Delta[1],\cdots,o_j^\Delta[i]) = \\ f(\chi_j(s^\Delta[i-1]), o_j^\Delta[1],\cdots,o_j^\Delta[i-1]) \times \\ \mathbb{P}(s^\Delta[i] | s^\Delta[i-1]) f(o_j^\Delta[i] | s^\Delta[i]). \end{aligned}$$

Iterating over n slots, the nodes $j \in \{1,2\}$ find $\tilde{\mathbf{s}}_j^\Delta = \arg\max_{\chi_j(s^\Delta[n])} \mathbb{P}(\chi_j(s^\Delta[n]) | \mathbf{o}_j)$.

D. Public Discussion

In this stage, legitimate nodes 1 and 2 agree on a key based on their location estimates $\tilde{\mathbf{s}}_j^\Delta$ after exchanging messages over the authenticated error-free public channel. First, we explain the process for no GLI. Due to the lack of angle information at the legitimate nodes, keys are generated solely from the nodes' quantized estimates $\tilde{\mathbf{d}}_j^\Delta$ of the relative distance $\mathbf{d}_{12}$, which is extracted from their location estimates $\tilde{\mathbf{s}}_j^\Delta$ as follows: The term $\tilde{\mathbf{s}}_j^\Delta$ can be written as $\tilde{\mathbf{s}}_j^\Delta = [\mathbf{l}_1^\Delta, \mathbf{l}_2^\Delta, \mathbf{l}_e^\Delta]$, and for any i, $\tilde{d}_j^\Delta[i] = \|l_1^\Delta[i] - l_2^\Delta[i]\|$. Since the nodes' mobility is not i.i.d., their locations, hence relative distances in the consequent slots are correlated with each other. Therefore, we only consider the relative change in distance, instead of the distance itself. First, the nodes convert their estimates of the relative change in distance to binary form as follows. Let $\kappa : \mathcal{Q}^\Delta \to \{0,1\}^m$, where $\mathcal{Q}^\Delta$ is the set of possible quantized distance differences. The mapping is one to one and order preserving. For instance, $\kappa(\tilde{d}_j^\Delta[i] - \tilde{d}_j^\Delta[i-1]) = [1\ 1\ \ldots 1]$ if $\tilde{d}_j^\Delta[i] - \tilde{d}_j^\Delta[i-1]$ attains the maximum possible value, i.e., if the legitimate nodes move farthest apart possible from each other in slot i, and $\kappa(\tilde{d}_j^\Delta[i] - \tilde{d}_j^\Delta[i-1]) = [0\ 0\ \ldots 0]$ if $\tilde{d}_j^\Delta[i] - \tilde{d}_j^\Delta[i-1]$ attains the minimum possible value, i.e., if the legitimate nodes move closest to each other possible in slot i. The number of digits m depends on the possible distance change combinations, which depends on the mobility model, and the choice of Δ. From these binary sequences, node $j \in \{1,2\}$ forms $\mathbf{v}_j \in \{0,1\}^{nm}$, where

$$\left[v_j[(i-1)m_1] \;\ldots v_j[im_1 - 1]\right] = \kappa(\tilde{d}_j^\Delta[i] - \tilde{d}_j^\Delta[i-1]).$$

For perfect GLI, the legitimate nodes also make use of their estimates of the angle information $\boldsymbol{\theta}_{12}$, which provides additional bits to their message sequences $\mathbf{v}_j$. The process is very similar to the no GLI case, hence is not covered here.

Next, the nodes apply Cascade reconciliation protocol [27] to agree on a secret key based on their nm bit binary sequences $\mathbf{v}_j$. Cascade is a two-way public discussion protocol which exchanges amount of information close to the theoretical bound when $\mathbf{v}_j$ are binary symmetric sources with crossover probability up to 15%. Here, we provide a brief sketch of how the protocol applies to our scenario. The protocol operates over several passes. In the first pass, binary sequences $\mathbf{v}_j$ are divided into n_1 blocks $\mathbf{u}_{j,0}[1]\ldots,\mathbf{u}_{j,0}[n_1]$ of size m_1 such that $n_1 m_1 = nm$, and

$$\mathbf{u}_{j,0}[i] \triangleq [v_j[(i-1)m_1] \;\cdots\; v_j[im_1 - 1]]$$

and

$$\mathbf{u}_{j,0} \triangleq [\mathbf{u}_{j,1}[1] \cdots \mathbf{u}_{j,1}[n_1]]\,.$$

Node 1, the master node, calculates parity bits $C_1[i]$ from each block $\mathbf{u}_{1,0}[i]$ as

$$C_1[i] = v_1[(i-1)m_1] \;\oplus \cdots \oplus v_1[im_1 - 1],$$

and communicates $[C_1[1]\cdots C_1[n]]$ to node 2 over the public channel. Node 2 similarly calculates the parity bits $C_2[i]$ from $\mathbf{u}_{2,0}[i]$. If the parity in block i does not match, i.e., $C_1[i] \neq C_2[i]$, then it indicates that there are odd number of errors in block i. In that case, a recursive protocol referred to in [27] as BINARY is executed, which is essentially recursively dividing block i to sub-blocks and comparing the parities of the sub-blocks until a bit in error is found. When all the blocks $1\ldots n_1$ are compared, they all contain even number of errors, and the first pass is over. In the subsequent passes $p > 1$, the sequences $\mathbf{u}_{j,p-1}$ are shuffled according to some random permutation function g such that

$$\mathbf{u}_{j,p} \triangleq g(\mathbf{u}_{j,p-1}),$$

and the parity exchange process on each block $\mathbf{u}_{j,p}[i]$, $i \in \{1\ldots n_p\}$ is similarly repeated. Note that, when an error is found and corrected in p'th pass, the blocks containing that corrected bit in the $p-1$ passes contain odd number of errors. Therefore, the parity exchange process is repeated on the smallest sub-block of the among those blocks. This process is repeated for P passes, where P depends on the bit mismatch rate of the initial sequences $\mathbf{v}_j$. At the end of the protocol, T bits is exchanged each way between the legitimate nodes,

where node j has sent bits $[C_j[1]\cdots C_j[T]]$. Due to the interactive nature of the protocol, the number T depends on the initial bit mismatch rate between the sequences $\mathbf{v}_1$ and $\mathbf{v}_2$, and the number of passes P.

In [27], it is suggested that the block size m_p in pass p is chosen such that $m_p = 2m_{p-1}$ for $p > 1$, and m_1 is chosen such that $\mathbb{P}(\mathbf{u}_{1,0}[i] \neq \mathbf{u}_{2,0}[i]) = 0.7$. Probability of error after the public discussion, $\mathbb{P}(\mathbf{u}_{1,P} \neq \mathbf{u}_{2,P})$, decays exponentially with number of passes P, which is chosen large enough such that the reliability constraint in Definition 2 is satisfied. For simplicity, we drop the number of iterations for the key sequences generated at the end of Cascade reconciliation protocol and denote the resulting key sequences with: $\mathbf{u}_j \triangleq \mathbf{u}_{j,P}$.

E. Privacy amplification

After the public discussion case, the legitimate nodes 1 and 2 end up with keys $\mathbf{u}_1$ and $\mathbf{u}_2$, respectively. Meanwhile, the eavesdropper also obtains a key sequence $\mathbf{u}_e$ that is correlated with the legitimate nodes' keys due to two reasons: The eavesdropper's observations $\mathbf{o}_e$ are correlated with the legitimate nodes' observations $\mathbf{o}_1$, $\mathbf{o}_2$, the parity bits exchanged during cascade protocol in public discussion phase reveals some information about the keys $\mathbf{u}_1$ and $\mathbf{u}_2$ to the eavesdropper. In the privacy amplification phase, the legitimate nodes will map their keys into a shorter sequence, $\mathbf{k}_1$ and $\mathbf{k}_2$, of key bits in such a way that the eavesdropper has no information on them. Privacy amplification is typically done by hash functions that have approximate universality properties [28]. Let H_{hash} denote the used hash function. In our algorithm, we use the SHA-256 [26] hash function for H_{hash}, i.e., $\mathbf{k}_1 = H_{hash}(\mathbf{u}_1)$, and $\mathbf{k}_2 = H_{hash}(\mathbf{u}_2)$, both of size nR.

Now, we explain the choice of rate R. We cannot explicitly find the *supremum* of rates R for which our key generation algorithm is perfectly reliable according to Definition 1, since calculation of the equivocation rate at the eavesdropper, given in equation (11) is not feasible. However, we assume that the eavesdropper follows a strategy that is better than the optimal strategy it can perform, as follows. In Localization phase, we assume that the eavesdropper also uses the Viterbi Algorithm to obtain the estimate $\tilde{\mathbf{s}}_e^{\Delta'}$ of the locations, and converts it to a bit sequence $\mathbf{v}_e$ of size nm. The public discussion phase consists of two stages. In the first stage, node $j \in \{1, 2\}$ obtains $\tilde{s}_j^{\Delta}$ based on the observations $\mathbf{o}_j$ and obtains the bit sequence $\mathbf{v}_j$. In the second stage, node 1 sends parity bits $[C_1[1], \cdots, C_1[T]]$ and node 2 feeds back parity bits $[C_2[1], \cdots, C_2[T]]$ as acknowledgments in the cascade algorithm and the nodes obtain bit sequences $\mathbf{u}_1$ and $\mathbf{u}_2$, both of size nm, where $\mathbf{u}_1 = \mathbf{u}_2$ with high probability. Note that, this approach is suboptimal compared to the soft decoding scheme in which the bit sequence $\mathbf{u}_2$ is decoded directly based on the observations $\mathbf{o}_2$ and the parity bits. Therefore, in our security analysis, we assume that the eavesdropper does not follow the suboptimal approach. Instead, we make the highly optimistic assumption for the eavesdropper that it corrects T bits that was in error; equal to the number of parity bits exchanged each way during cascade protocol.

In the privacy amplification step, the rate of hashing R is chosen as follows. Due to the privacy amplification result in [28], it is sufficient to choose the rate R less than the equivocation rate (prior to privacy amplification) at the eavesdropper to avoid an information leakage to the eavesdropper at a positive rate. Due to quantization applied at the eavesdropper, the equivocation rate of the bit sequence $\mathbf{u}_1$ becomes

$$H\left(\mathbf{u}_1|\tilde{\mathbf{s}}_e^{\Delta'}, \{C_1[t], C_2[t]\}_{t=1}^{T}\right) \geq H(\mathbf{u}_1|\mathbf{u}_e) - T, \quad (16)$$

where (16) follows from the fact that public broadcast of the messages $\{C_1[t], C_2[t]\}_{t=1}^{T}$ can at most reveal T bits from $\mathbf{u}_1$. Therefore, it suffices to choose the rate R as [3]

$$R = H(\mathbf{u}_1|\mathbf{u}_e) - T - \delta.$$

to satisfy the security constraint in Definition 2. In the privacy amplification stage of our scheme, we choose T large enough to achieve a given constraint $\text{BMR}_j < \epsilon$, but not too large and make the key rate R too small. In Section V, we derive fundamental limits on the achievable key rate, subject to perfect reliability and compare the performance of our algorithm with the bounds in Section VI.

Finally, for the randomness of the generated keys, we use the NIST test suite, and perform the randomness tests of the generated key sequence $\mathbf{k}_1$ and $\mathbf{k}_2$.

V. Theoretical Performance Limits

In this section, we provide the theoretical bounds on the achievable key rate with perfect reliability. To evaluate these bounds, we assume an idealized system by ignoring the issues associated with quantization, cascade reconciliation protocol, and SHA-based privacy amplification. Thus, these bounds are valid for *any* key generation scheme.

A. Bounds on the Achievable Key Rate

In this section, we establish upper and lower bounds on the key bits achievable through public discussion, with and without GLI.

[3]Note that, for $n \gg 1$, $H(\mathbf{u}_1|\mathbf{u}_e)$ can be approximately evaluated as follows. Let $\mathbf{u}_e$ be formed by passing $\mathbf{u}_1$ through a binary symmetric channel, with crossover probability BMR_e, identical to the bit mismatch rate of the eavesdropper, i.e., $\text{BMR}_e = \frac{\sum_{i=1}^{nm} \mathbf{1}(u_1[i] \neq u_e[i])}{nm}$. Then, $H(\mathbf{u}_1|\mathbf{u}_e) \approx nm(1 - \text{BSC}(\text{BMR}_e))$, where $\text{BSC}(\text{BMR}_e)$ denotes the capacity of a binary symmetric channel with crossover probability of BMR_e.

Algorithm 1 Key Generation From Localization

Step 0: Quantization
$\psi(\cdot) : \{l_j[i]\} \to \{1 \dots M\}^2$
$l_j^{\Delta}[i] \leftarrow \psi(l_j[i])$
$s_j^{\Delta}[i] \leftarrow [l_1^{\Delta}[i], l_2^{\Delta}[i], l_e^{\Delta}[i]]$
Step 1: Opportunistic Beacon Exchange : Forward Algorithm
$(\mathbf{o}_1, \mathbf{o}_2, \mathbf{o}_e) \leftarrow$BEACON
Step 2: Localization : Viterbi Algorithm
for node $j \in \{1, 2\}$ **do**
  for slot $i = 1 : n$ **do**
    for $s^{\Delta}[i-1] \in \{1 \dots M\}^6$ **do**
      for $s^{\Delta}[i] \in \{1 \dots M\}^6$ **do**
        if $f(o_j[1], \dots, o_j[i], \chi_j(s^{\Delta}[i-1]), s^{\Delta}[i]) > f(o_j[1], \dots, o_j[i], \chi_j(s^{\Delta}[i]))$ **then**
          $\chi_j(s^{\Delta}[i]) \leftarrow (\chi_j(s^{\Delta}[i-1]), s^{\Delta}[i])$
        end if
      end for
    end for
  end for
  $\tilde{s}_j^{\Delta}[n] \leftarrow \arg\max_{\chi_j(s^{\Delta}[n])} f(\chi_j(s^{\Delta}[n]), \mathbf{o}_j^{\Delta})$
end for
Step 3: Public Discussion: Cascade Protocol
for slot $i = 1 : n$ **do**
  $v_j[i] \leftarrow \kappa(\tilde{d}_j^{\Delta}[i] - \tilde{d}_j^{\Delta}[i-1])$
end for
$(\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_e) \leftarrow$ CASCADE$(\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_e)$
Step 4: Privacy Amplification
$\mathbf{k}_j \leftarrow H_{hash}(\mathbf{u}_j),\ j \in \{1, 2\}$

Algorithm 2 Opportunistic Beacon Exchange

BEACON:
$j \leftarrow$ Master Node
CTR$\leftarrow 0$
$\mathbb{P}(s_1^{\Delta}[0]) \leftarrow 1/M^6,\ \forall s_1^{\Delta}[0] \in \{1 \dots M\}^6$
for slot $i = 1 : n$ **do**
  $\zeta \leftarrow 0$
  for $s^{\Delta}[i-1] \in \{1 \dots M\}^6$ **do**
    for $s^{\Delta}[i] \in \{1 \dots M\}^6$ **do**
      $x_1 \leftarrow \mathbf{1}\left(\gamma(d_{12}[i]) > A[i] + B[i]|s^{\Delta}[i]\right)$
      $x_2 \leftarrow f(o_j[1], \dots, o_j[i-1], s^{\Delta}[i-1])$
      $x_3 \leftarrow \mathbb{P}(s^{\Delta}[i]|s^{\Delta}[i-1])$
      $\zeta \leftarrow \zeta + x_1 x_2 x_3$
    end for
  end for
  if $\zeta < \tau$ **or** CTR $\geq c$ **then**
    NODE 1 TX BEACON
    NODE 2 TX BEACON
    $o_j[i] \leftarrow (\hat{d}_j[i], \Delta)$
    CTR $\leftarrow 0$
  else
    NODE 1 SILENT
    NODE 2 SILENT
    $o_j[i] \leftarrow \emptyset$
    CTR $\leftarrow$ CTR+1
  end if
end for

Theorem 1: A lower bound R_L, and an upper bound R_U on the perfectly-reliable key rate achievable through public discussion are

$$R_L = \max\left\{ \lim_{n\to\infty} \frac{1}{n} \left[I(\mathbf{o}_1; \mathbf{o}_2) - I(\mathbf{o}_1; \mathbf{o}_e)\right]^+, \lim_{n\to\infty} \frac{1}{n} \left[I(\mathbf{o}_2; \mathbf{o}_1) - I(\mathbf{o}_2; \mathbf{o}_e)\right]^+ \right\} \quad (17)$$

and

$$R_U = \lim_{n\to\infty} \frac{1}{n} \min\left\{I(\mathbf{o}_1; \mathbf{o}_2), I(\mathbf{o}_1; \mathbf{o}_2|\mathbf{o}_e)\right\} \quad (18)$$

respectively, where the observations $\mathbf{o}_1, \mathbf{o}_2$ and $\mathbf{o}_e$ are as given in Table II for different possibilities of GLI. The theorem follows[4] from Theorem 4 in [16], which generalizes Maurer's results on secret key generation through public discussion [1], to non-i.i.d. settings. Note that tighter bounds exist in the literature [2], [3], however we use the above bounds, since they provide much clearer insights into our systems due to their simplicity.

Note that for the special case where node locations $(l_1[i], l_2[i], l_e[i])$ are i.i.d., it is clear that the distances $(d_{12}[i], d_{1e}[i], d_{2e}[i])$, angles $(\phi_{12}[i], \phi_{1e}[i], \phi_{2e}[i])$, and observations $(o_1[i], o_2[i], o_e[i])$ are also i.i.d.. Hence we can safely drop the index i, and denote the joint probability density function of observations as $f(o_1, o_2, o_e)$. Therefore, the conditioning on the past and future observations in R_L and R_U disappear, and the lower and upper bound expressions reduce to

$$R_L = \max\Big(\left[I(o_1; o_2) - I(o_1; o_e)\right]^+, \left[I(o_1; o_2) - I(o_2; o_e)\right]^+ \Big) \quad (19)$$

$$R_U = \min\left(I(o_1; o_2), I(o_1; o_2|o_e)\right), \quad (20)$$

respectively.

B. Beacon Power Asymptotics

In this part, we analyze the beacon power asymptotics of the system. We show that, if the eavesdropper does not observe the angle, i.e., $\hat{\phi}_e = \emptyset$, then R_L increases unboundedly with the beacon power P, which indicates

[4]Theorem 4 of [16] provide general upper and lower bounds including the case where the source processes are not ergodic. In our system model, $\mathbf{o}_1$, $\mathbf{o}_2$ and $\mathbf{o}_e$ are ergodic processes, hence they are information stable, therefore these lower and upper bounds reduce to (17) and (18), respectively [15].

that arbitrarily large secret key rates can be obtained. However, when eavesdropper observes the angle information, then R_U remains bounded, which indicates that the advantage gained by increasing beacon power is rather limited. Hence, we show a phase-transition phenomenon with the angle observations. Even with a highly noisy angle observation, as long as $I(\hat{\boldsymbol{\phi}}_e;\boldsymbol{\phi}_e) > 0$, the key rate does not grow unboundedly with the beacon power. To clearly illustrate our insights, we present our results for the no GLI scenario. However, the same conclusion holds for the perfect GLI case as well.

Theorem 2: When the eavesdropper obtains angle information, i.e., $I(\hat{\boldsymbol{\phi}}_e;\boldsymbol{\phi}_e) > 0$,

$$\lim_{P\to\infty} R_U < \infty. \tag{21}$$

The proof is in Appendix B, where we show that $\lim_{P\to\infty} R_U \leq \eta$, where

$$\begin{aligned}\eta = \frac{1}{2}\log\Bigg\{ & 2\pi\mathbb{E}\Bigg[\frac{\rho_e}{d_{12}^2}\Bigg(\frac{d_{12}^2\rho_1}{\rho_e}\gamma(d_{12}) \\ & + 4(d_{1e}+d_{2e})^2(\sqrt{\gamma(d_{1e})}+\sqrt{\gamma(d_{2e})})^2 \\ & + (4d_{1e}d_{2e}+64(d_{1e}d_{2e})^2)\gamma_\phi(d_{1e},d_{2e}) \\ & + 8(d_{1e}+d_{2e})d_{1e}d_{2e}\big(\sqrt{\gamma(d_{1e})} \\ & + \sqrt{\gamma(d_{2e})}\big)\sqrt{\gamma_\phi(d_{1e},d_{2e})} \\ & + 64(d_{1e}+d_{2e})^2(\gamma(d_{1e})+\gamma(d_{2e}))\Bigg)\Bigg]\Bigg\} \\ & - \frac{1}{2}\mathbb{E}\Big[\log\left(2\pi\rho_1\gamma(d_{12})\right)\Big].\end{aligned} \tag{22}$$

The parameter η remains finite as long as the distances take on values in some bounded range $[d_{\min}, d_{\max}]$ with probability 1. Therefore, the secret key rate remains bounded.

Theorem 3: When the eavesdropper does not obtain any angle information, i.e., $I(\hat{\boldsymbol{\phi}}_e;\boldsymbol{\phi}_e) = 0$,

$$\begin{aligned}\lim_{P\to\infty}\frac{R_L}{\frac{1}{2}\log(P)} &= \lim_{P\to\infty}\frac{R_U}{\frac{1}{2}\log(P)} \\ &= 1.\end{aligned}$$

The proof is provided in Appendix B. Theorem 3 implies that, without the angle observation at the eavesdropper, an arbitrarily large key rate can be achieved with sufficiently large beacon power P. However, the key rate increases with $\log(P)$, which means that increasing the beacon power would provide diminishing returns. Also, note that, apart from the beacon power, there are other practical factors limiting the key rate, such as biased observations. We study such limitations in Appendix C.

VI. Numerical Evaluations

In this section, we evaluate the key rate performance of our key generation algorithm, and compare with the theoretical bounds on the secret key rates using Monte Carlo simulations. We also study the theoretical performance gain of the opportunistic beacon exchange strategy used in part of our algorithm. First, we briefly explain the setup, then provide the results.

Setup: An $(M \times M)$ discrete 2-D grid simulates a city with M blocks, that covers a square field of area A^2, such that for any $j \in \{1, 2, e\}$, $i \in \{1, \ldots, n\}$, $l_j[i] = [x\ y] \in \{\frac{A}{M}, \ldots, M\frac{A}{M}\} \times \{\frac{A}{M}, \ldots, M\frac{A}{M}\}$. Node mobilities are Markov, and characterized by parameter B, where

$$\mathbb{P}\big(l_j[i] = [x\ y] \mid l_j[i-1] = [x'\ y']\big) = \begin{cases} \frac{1}{(B+1)^2} \text{ if } & |x-x'| \leq \frac{AB}{M} \\ & |y-y'| \leq \frac{AB}{M} \\ 0 & \text{otherwise} \end{cases}$$

For no GLI, the nodes' observations are as defined in (1)-(3), where we assume $\gamma(d) = 0.1 + d^2$, and

$$\gamma_\phi(d_{1e}, d_{2e}) = \pi - \frac{\pi}{1.1 + (d_{1e}^2 + d_{2e}^2)},$$

such that both parameters are strictly increasing functions of the distances.[5] For perfect GLI, the angle observations of the nodes are as defined in (4) and (5), where

$$\gamma_\phi(d_{je}) = \pi - \frac{\pi}{1.1 + (d_{je})^2}$$

for $j \in \{1, 2\}$. The distance observations are the same as in no GLI case. For both cases, the node capability parameters $\rho_1 = \rho_2 = \rho_e = 1$ unless otherwise stated. The theoretical key rates in Section V converge as n goes to infinity, therefore they are calculated for large enough n, using the forward algorithm procedure described Section IV.

Results: Due to computational limitations[6], we consider examples in which $M \leq 11$, and $B \leq 3$. Note that this choice limits the maximum achievable secret key rate. For instance, for the choice of $B = 1$, due to the limited mobility of the nodes, there are 13 different possible distance combinations. Consequently, a key rate of $\log 13$ is an absolute upper bound on the key rate for no GLI even in the case when the eavesdropper does not obtain any distance or angle observation. Note that, the actual key rate can be much lower than $\log 13$ due to the eavesdropper's observations. In the light of this, we

[5]Since $\phi_e \in [0, \pi]$, the angle observation error variance cannot diverge with distance, and in our model, the variance is chosen to be upper bounded by $\pi/1.1$. To avoid zero error variances at zero distance, we introduce a 0.1 offset to numerator and denominator of γ and γ_ϕ, respectively.

[6]Although the forward algorithm makes the calculation of the bounds possible, since the complexity of forward algorithm scales with the square of the available states, which is equal to M^6, it is not computationally feasible to calculate the bounds for large values of M, B.

would like to point out that, the main objective of our initial set of simulations is to provide insights into the relationships between the basic parameters of the system, to compare the performance of the opportunistic key generation scheme with the maximum achievable key rate, and to illustrate the tradeoffs involved. In reality, the grid sizes will be much larger and the mobility pattern typically allows for a richer variety (and hence a larger entropy rate), depending on the speed and the maneuvering capabilities of the nodes. Note that, our key rate plots are as a function of normalized beacon power P/σ_0^2, where σ_0^2 denotes the variance of distance observations $\hat{d}_j[i]$ of legitimate nodes at unit distance.

First, we provide the performance results of our key generation algorithm. In Figure 4, we plot the key rate achieved with our algorithm with respect to the normalized beacon power P/σ_0^2 for $M = 5$, $A = 5$, and $B = 1$. We show that, even in this grid with a small number of possible locations, we can generate (ϵ, δ)-reliable key bits comparable with the theoretical capacity bounds provided in Section V, for $\epsilon = \delta = 10^{-3}$. Note that the key rate starts to decrease at a certain beacon power, beyond which the rate of information accumulation at the eavesdropper exceeds that at the legitimate nodes. Also, we emphasize that the lower bound and the upper bound provided in Figure 4 are analytically proven bounds on key capacity, where the lower bound is achieved by using random coding arguments which are not feasible to implement due to computational complexity. Although our algorithm performs worse than the theoretical lower bound, it is implemented using tools that are feasible to use, such as viterbi algorithm, cascade algorithm, etc. In Table III, we provide the results of the NIST randomness tests. Here, a value greater than 0.01 is considered as a pass [25].

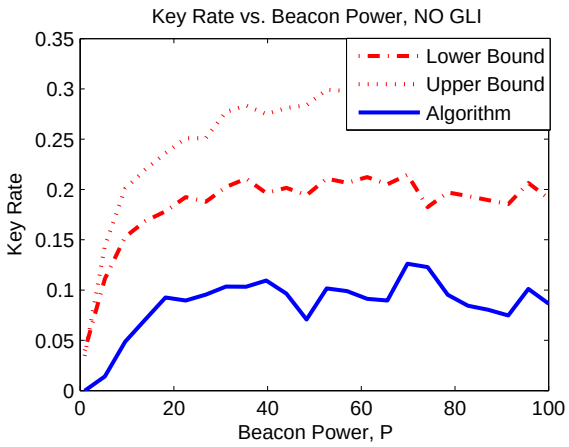

Fig. 4: Comparison of theoretical key capacity limits and key generation algorithm vs normalized beacon power P/σ_0^2, no GLI

Test type	result
Frequency	0.534146
BlockFrequency	0.911413
CumulativeSums	0.534146
Rank	0.066882
FFT	0.350485
LinearComplexity	0.122325

TABLE III: Randomness test results for the key generation algorithm

Then, we analyze the effect of the different grid size, field area and GLI on the theoretical key rates. In Figures 5 and 6, we plot the bounds on the achievable key rate with respect to the normalized beacon power P/σ_0^2 for different grid size M for no GLI and perfect GLI cases, respectively. We assumed a constant ratio of field size and grid size, $A/M = 1$, and considered $B = 1$. We can see that, there is a diminishing return on the increased power levels for the achievable key rate. Furthermore, we can see that increasing the field area A^2 has a negative impact on the key rate despite the increase in M, which is due to the fact that the common information of the legitimate nodes decreases as a result of increase in their observation error variance. Next, in Figures 7 and 8, we plot the bounds with respect to beacon power P, for different step size $B = 1$ for no GLI and perfect GLI cases, respectively. We assumed $M = 5$ for the no GLI case, and $M = 7$ for perfect GLI case, and in both cases, the ratio of field size and grid size is constant, such that $A/M = 1$. We can clearly see the positive effect of the increased step size on the secret key rate. This is due to the increase in different distance combinations that are possible.

Next, for no GLI, we evaluate the theoretical per-

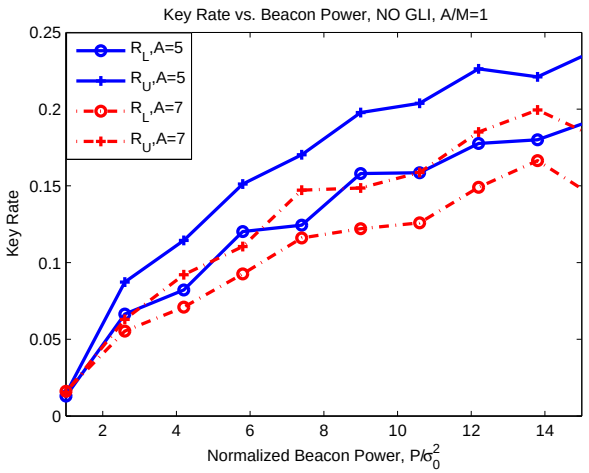

Fig. 5: Upper and lower bounds for no GLI vs normalized beacon power P/σ_0^2, for different M, $B = 1$, $A/M = 1$

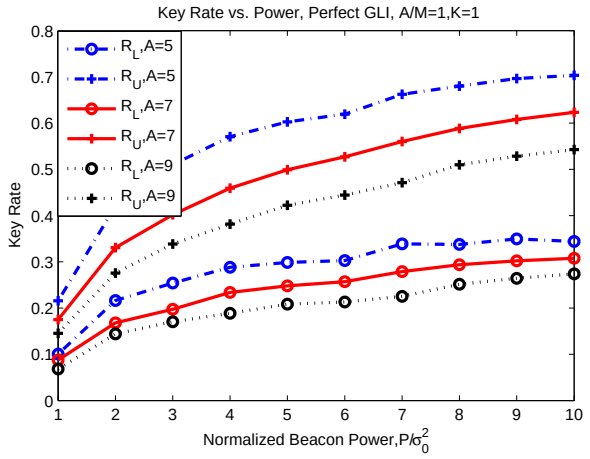

Fig. 6: Upper and lower bounds for perfect GLI vs normalized beacon power P/σ_0^2, for different M, $B = 1$, $A/M = 1$

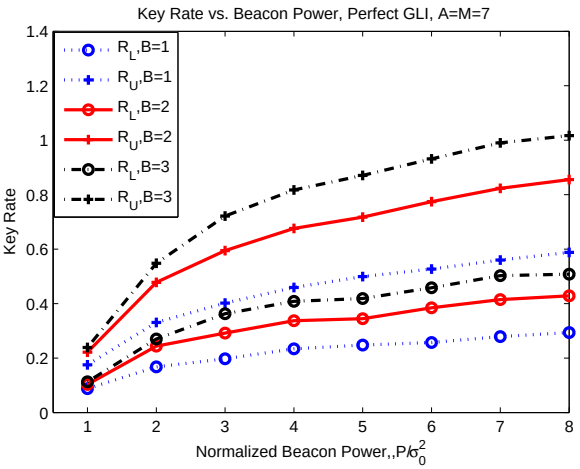

Fig. 8: Upper and lower bounds for perfect GLI vs normalized beacon power P/σ_0^2, $M = A = 7$, for different B

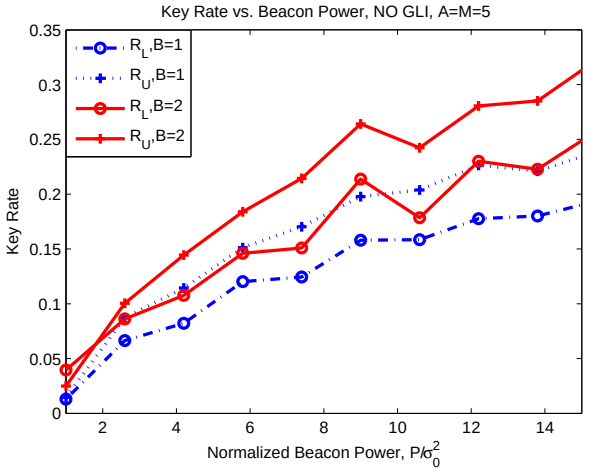

Fig. 7: Upper and lower bounds for no GLI vs normalized beacon power P/σ_0^2, $M = A = 5$, for different B

formance of opportunistic beacon exchange scheme as well as the impact of the eavesdropper mobility scheme, both described in Section IV. First, we compare the performance of our proposed opportunistic beacon exchange scheme with the non-opportunistic counterpart, which transmits out beacons in each time slot. We show that, even under a pessimistic scenario for the legitimate nodes, non-zero secret key rates can be achieved by our opportunistic scheme, which would not be possible with the non-opportunistic case: We assume that node e is more capable such that $\rho_1 = \rho_2 = 1$ and $\rho_e = 0.6$, which can model the case where node e is equipped with more antennas compared to the legitimate nodes. Furthermore, node e stays fixed at the center of the $M \times M$ grid, for $M = 7$ and $A = 5$ and $B = 1$. Since the observation noise variance is an increasing function of the node distances, this also gives node e a geographic advantage over the legitimate nodes 1 and 2. We can see from Figure 9 that secret key rate decays to 0 with the non-opportunistic scheme. On the other hand, non-zero secret key rates can be achieved with our opportunistic strategy outlined in Section IV, for parameters $\tau = 0.5$ and $c = 4$. On the same figure, we also plot the achievable key rates for the genie-aided scheme, which has the reach to the perfect side information on whether the legitimate nodes have a geographical advantage or not at any given point in time. With such side information, the key rate is roughly doubled compared to our opportunistic scheme. Note that our algorithm obtains information on the presence of a geographical advantage, based solely on the beacon observations. One of the issues is that, when the two legitimate nodes skip beacon transmissions, their information on each other's location becomes more degraded, hence they cannot predict whether they still keep the geographic advantage compared to the eavesdropper. Despite the fact that our algorithm skips on the average 69% of the beacon transmissions due to a predicted geographic disadvantage, it is remarkable that roughly half the key rate is achievable with our scheme compared to the case with the genie-aided perfect side information.

Finally, we analyze the effect of eavesdropper mobility on the achievable key rate. In Figure 10, for $M = 7$, $A = 5$ and $B = 1$, we plot the secret key rate bounds versus beacon power for the cases where the eavesdropper i) follows the random mobility pattern described in the setup with parameter $B = 1$, ii) stays at the origin, and iii) follows the man in the middle strategy described in Section III-C, i.e., moves to the mid point

of its location estimates of nodes 1 and 2. We can see that, compared to following a random mobility pattern, the eavesdropper can reduce the achievable secret key rate significantly by following this strategy. Also, it is notable that the eavesdropper can significantly reduce the key rate by simply staying static at a certain favorable location, rather than moving randomly. Note that, in practice this may not be feasible for the eavesdropper, since, by staying put, it will lose connection completely with the legitimate nodes in a large region.

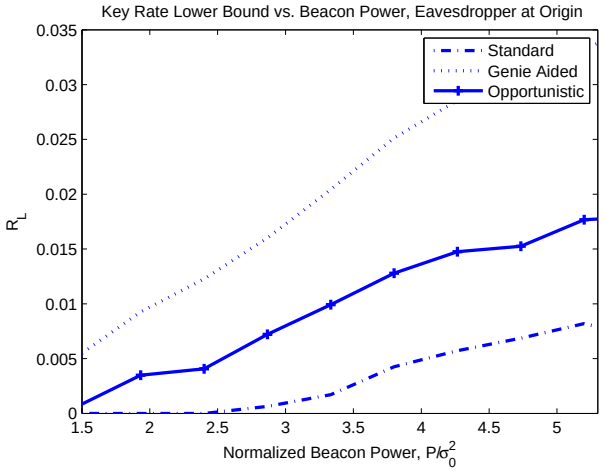

Fig. 9: Opportunistic beacon exchange, no GLI

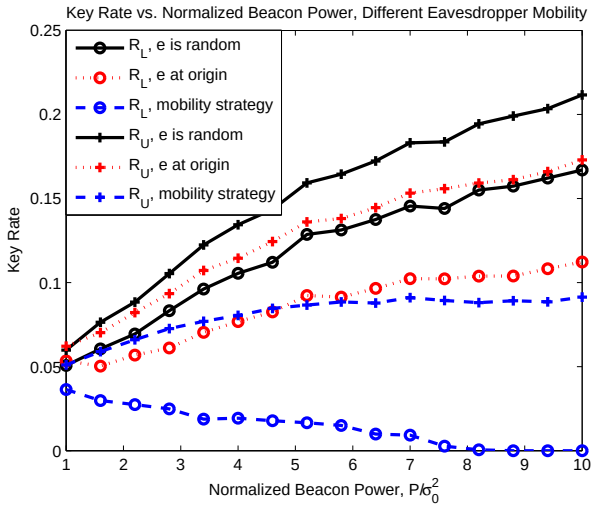

Fig. 10: Effect of eavesdropper mobility on the key rate

VII. Conclusion

In this paper, we developed a four stage algorithm that generates keys based on the relative localization information between legitimate nodes in mobile wireless networks. The first stag In the first stage, legitimate nodes generate relative localization information by opportunistically exchanging beacons whenever the legitimate nodes sense a geographic advantage compared to the eavesdropper. In the second stage, the nodes perform localization, and in the third stage, the nodes' relative distance estimates are converted to a binary sequence, out of which the nodes agree on some initial key bits by public discussion. Finally, privacy amplification is performed on the key bits to obtain the final key with a low bit mismatch rate at the legitimate nodes as well as a low information leakage rate to the eavesdropper. We also studied the information theoretic limits of secret key generation, and characterized lower and upper bounds of key rates utilizing results from the source model of secrecy, for the cases in which the nodes are/are not capable of observing their global locations. Furthermore, we studied the beacon power asymptotics, and showed that when the eavesdropper cannot observe the angle information, the secret key rate grows unboundedly, whereas with an angle observation at eavesdropper, key rate remains bounded. We showed that a secret key rate, identical to half of that achievable with perfect side information on whether the legitimate nodes have a geographical advantage can be obtained with our opportunistic strategy. This is highly significant, since we show that it is not possible to achieve a non-zero key rate with a non-opportunistic strategy. Then, we studied mobility strategies for the eavesdropper to minimize the secret key rate. Our current investigations are mainly focused on 1) common secret key generation among multiple nodes in a wireless network, 2) application to wideband localization, and 3) practical applications on high beacon SNR.

Appendix A
On opportunistic beacon exchange

We do not directly use (12) for beacon transmission decisions due to certain challenges. Here, we address them, and justify why we use (13) instead. The first issue is that it is difficult to verify Condition (12). To see whether there exists a valid probability density function $\tilde{f}$ that satisfies (12), we can pose the problem as that of calculus of variations:

$$\mu = \min_{\tilde{f}} \left| f(\hat{d}_1[i]|d_{12}[i]) - \int_{x=(\hat{d}_{1e}[i],\hat{d}_{2e}[i],\hat{\phi}_e[i])} f(x|d_{12}[i])\tilde{f}(\hat{d}_1[i]|x)\mathrm{d}x \right|$$

$$\text{subject to : } \int \tilde{f}(u)\mathrm{d}u = 1.$$

If $\mu = 0$, then the legitimate nodes' observations are stochastically degraded version of the eavesdropper's observations. However, due to the fact

that there may exist no closed form expression for $f(\hat{d}_{1e}[i], \hat{d}_{2e}[i], \hat{\phi}_e[i]|d_{12}[i])$, this problem can be highly complex. Instead, in our algorithm, the legitimate nodes make their decisions based on an approximate version of (12) at the expense of some loss in the key rate. Define $\hat{d}_e[i]$ as

$$\hat{d}_e[i] = \sqrt{\left[\hat{d}_{1e}[i]^2 + \hat{d}_{2e}[i]^2 - 2\hat{d}_{1e}[i]\hat{d}_{2e}[i]\cos(\hat{\phi}_e[i])\right]^+}, \tag{23}$$

which corresponds to the cosine law estimate of $d_{12}[i]$ of the eavesdropper. Through a sequence of approximations on $\hat{d}_e[i]$ as described in Appendix A-A, we end up with

$$\hat{d}_e^*[i] = d_{12}[i] + w_e[i], \tag{24}$$

where $w_e[i] \sim \mathcal{N}\left(0, \frac{\rho_e(A[i]+B[i])}{P}\right)$, such that

$$A[i] = \frac{\left(d_{1e}[i] - d_{2e}[i]\cos(\phi_e[i])\right)^2 \gamma(d_{1e}[i])}{d_{12}[i]^2} + \frac{\left(d_{2e}[i] - d_{1e}[i]\cos(\phi_e[i])\right)^2 \gamma(d_{2e}[i])}{d_{12}[i]^2}$$

is the uncertainty that comes from the distance observation errors, and

$$B[i] = \frac{(d_{1e}[i]d_{2e}[i]\sin(\phi_e[i]))^2 \gamma_\phi(d_{1e}[i], d_{2e}[i])}{d_{12}[i]^2}$$

is the uncertainty that comes from the angle estimate error. Note that the idea behind the described approximation is linearization of $\hat{d}_e[i]$ and hence the approximation becomes more and more accurate as the beacon power increases (i.e., in the high signal to noise ratio regime).

In our algorithm, the legitimate nodes use the term $\hat{d}_e^*[i]$ for beacon transmission decisions. Clearly, $d_{12}[i] \to (\hat{d}_{1e}[i], \hat{d}_{2e}[i], \hat{\phi}_e[i]) \to \hat{d}_e^*[i]$ forms a Markov chain. Consequently, when $\hat{d}_1[i]$ and $\hat{d}_2[i]$ are stochastically degraded versions of $\hat{d}_e^*[i]$, they are also stochastically degraded versions of the eavesdropper observations $(\hat{d}_{1e}[i], \hat{d}_{2e}[i], \hat{\phi}_e[i])$, hence the condition (12) is satisfied. Since the legitimate nodes' observations follow the distributions

$$\hat{d}_1[i] \sim \mathcal{N}\left(d_{12}[i], \frac{\gamma(\rho_1 d_{12}[i])}{P}\right)$$
$$\hat{d}_2[i] \sim \mathcal{N}\left(d_{12}[i], \frac{\gamma(\rho_2 d_{12}[i])}{P}\right),$$

the condition

$$\rho_{\max}\gamma(d_{12}[i]) > \rho_e(A[i] + B[i]) \tag{25}$$

would be sufficient to verify that the actual node measurement is more degraded than the eavesdropper measurement[7]. Note that the legitimate nodes cannot make use of (25) for beacon transmission decisions directly, since they only have the statistics of the eavesdropper location, and they do not know the parameters $A[i]$, $B[i]$ and $d_{12}[i]$ exactly. However, using the statistical knowledge, they can calculate the probability of event (25), conditioned on their observations, which is (13). Therefore, (13) is used as a basis for beacon transmission decisions.

A. Linear Approximation for $\hat{d}_e$

In this part, we explain how we obtain $\hat{d}_e^*[i]$ from $\hat{d}_e[i]$ via a sequence of linear approximations. In what follows, we drop the time index $[i]$ for simplicity.

$$\begin{aligned}
\hat{d}_e &= \Bigg(\Big[(d_{1e}+w_{1e})^2 + (d_{2e}+w_{2e})^2 - \\
&\quad 2(d_{1e}+w_{1e})(d_{2e}+w_{2e})\cos(\phi_e + w_{\phi_e})\Big]^+\Bigg)^{0.5} \\
&\approx \Bigg(\Big[d_{1e}^2 + d_{2e}^2 + 2d_{1e}w_{1e} + 2d_{2e}w_{2e} \\
&\quad - 2d_{1e}d_{2e}\cos(\phi_e + w_{\phi_e}) - 2d_{1e}w_{2e}\cos(\phi_e + w_{\phi_e}) \\
&\quad - 2d_{2e}w_{1e}\cos(\phi_e + w_{\phi_e})\Big]^+\Bigg)^{0.5} \qquad (26) \\
&\approx \Bigg(\Big[d_{12}^2 + 2d_{1e}d_{2e}\sin(\phi_e)w_{\phi_e} + \\
&\quad 2w_{1e}(d_{1e} - d_{2e}\cos\phi_e) + \\
&\quad 2w_{2e}(d_{2e} - d_{1e}\cos\phi_e)\Big]^+\Bigg)^{0.5} \qquad (27) \\
&\approx d_{12} + \frac{1}{d_{12}^2}\Big(d_{1e}d_{2e}\sin(\phi_e)w_{\phi_e} + \\
&\quad w_{1e}(d_{1e} - d_{2e}\cos\phi_e) + w_{2e}(d_{2e} - d_{1e}\cos\phi_e)\Big) \qquad (28) \\
&= d_{12} + w_x, \qquad (29)
\end{aligned}$$

where (26) follows from omitting the higher order terms $(w_{1e}^2 + w_{2e}^2 + 2w_{1e}w_{2e}\cos(\phi_e + w_{\phi_e}))$, since their variances scale with $O(\frac{1}{P^2})$; (27) follows from the approximation

$$\begin{aligned}
cos(\phi_e + w_{\phi_e}) &= \cos(\phi_e)\cos(w_{\phi_e}) - \sin(\phi_e)\sin(w_{\phi_e}) \\
&\approx \cos(\phi_e) - w_{\phi_e}\sin(\phi_e),
\end{aligned}$$

which becomes accurate as $w_{\phi_e} \searrow 0$; and (28) follows from the linear approximation $\sqrt{1+x} \approx 1 + \frac{x}{2}$ for $x \ll 1$, which is accurate for high signal to noise ratio, i.e., w_{ϕ_e}, w_{1e}, and w_{2e} are all small (close to 0) with high

[7]Note however that converse is not true since $\hat{d}_{\tilde{e}}[i]$ is not a sufficient statistic of $(\hat{d}_{1e}[i], \hat{d}_{2e}[i], \hat{\phi}_e[i])$.

probability. Note that, the overall noise term follows the distribution $w_x \sim \mathcal{N}\left(0, \frac{\rho_e(A+B)}{P}\right)$.

APPENDIX B
PROOFS OF THEOREMS IN SECTION V-B

A. Proof of Theorem 2

We first provide several lemmas that will be useful when proving the theorem.

Lemma 1: Let x and y be random variables. Then,

$$\mathbb{V}ar(x+y) \leq 2\mathbb{V}ar(x) + 2\mathbb{V}ar(y). \tag{30}$$

If x and y are independent, then

$$\mathbb{V}ar(x+y) = \mathbb{V}ar(x) + \mathbb{V}ar(y). \tag{31}$$

Proof: When x and y are not independent,

$$\begin{aligned}\mathbb{V}ar(x+y) &= \mathbb{V}ar(x) + \mathbb{V}ar(y) + 2\mathbb{C}ov(x,y)\\ &\leq \mathbb{V}ar(x) + \mathbb{V}ar(y) + 2\sqrt{\mathbb{V}ar(x)\mathbb{V}ar(y)}\\ &\leq 2\mathbb{V}ar(x) + 2\mathbb{V}ar(y). \end{aligned}\tag{32}$$

where (32) follows from the fact that $\mathbb{V}ar(x)+\mathbb{V}ar(y) \geq 2\sqrt{\mathbb{V}ar(x)\mathbb{V}ar(y)}$. When x and y are independent, $\mathbb{C}ov(x,y) = 0$, implying the result. ■

Lemma 2: Let x be a random variable such that $\mathbb{E}[x] \geq \mu$, where $\mu > -1$. Let $\alpha = \frac{\sqrt{1+\mu}}{1+\mu}$. Then, $\mathbb{V}ar(\sqrt{[1+x]^+}) \leq \mathbb{V}ar(\alpha x)$.

Proof: Assume $\mathbb{E}[x] = \mu'$, where $\mu' \geq \mu$. Let $\alpha' = \frac{\sqrt{1+\mu'}}{1+\mu'}$. Let us define $f_1(x) \triangleq \sqrt{[1+x]^+}$, and $f_2(x) \triangleq \alpha'(1+x)$. Note that,

$$\begin{aligned}\mathbb{V}ar(\sqrt{[1+x]^+}) &= \mathbb{V}ar(f_1(x))\\ &\leq \mathbb{E}\big[(f_1(x) - \mathbb{E}[f_2(x)])^2\big]\end{aligned}$$

since the centralized second moment is minimized around the mean. Also,

$$\begin{aligned}\mathbb{V}ar(\alpha x) &\geq \mathbb{V}ar(\alpha' x)\\ &= \mathbb{V}ar(f_2(x))\end{aligned}$$

since $\mu' \geq \mu$, and $\alpha' \leq \alpha$. Therefore, it suffices to show that $\forall x$,

$$|f_1(x) - \mathbb{E}[f_2(x)]| \leq |f_2(x) - \mathbb{E}[f_2(x)]| \tag{33}$$

$$= |f_2(x) - \sqrt{1+\mu'}|. \tag{34}$$

holds.

i) First note that,

$$f_1(\mu') = f_2(\mu') = \sqrt{1+\mu'},$$

Therefore, the condition (34) is satisfied for $x = \mu'$.

ii) For $x > \mu'$,

$$\begin{aligned}f_1(x) &\leq f_1(\mu') + f_1'(\mu')(x-\mu') \qquad (35)\\ &\leq \sqrt{1+\mu'} + \alpha(x-\mu')\\ &= f_2(x)\end{aligned}$$

where $f_1'(\mu')$ is the first derivative of $f_1(x)$ at point $x = \mu'$. (35) follows from the fact that $f_1(x)$ is a strictly concave function in the interval $[-1\ \infty)$. Therefore, condition (34) is satisfied for $x > \mu'$.

iii) Combining the facts that $f_1(x)$ is a strictly concave function of x in the interval $[-1\ \infty)$; $f_2(x)$ is linear; $f_1(-1) = f_2(-1)$; and $f_1(\mu') = f_2(\mu')$, we can see that $\sqrt{1+\mu'} > f_1(x) \geq f_2(x)$ when $-1 < x < \mu'$. Therefore, condition (34) is satisfied for $-1 < x < \mu'$.

iv) When $x < -1$, $f_1(x) = 0$ and $f_2(x) < 0$, therefore, condition (34) is satisfied. This concludes the proof. ■

Lemma 3: Let x, y be random variables. Then,

$$\mathbb{V}ar\left(\mathbb{E}\left[1 - \sqrt{(1+x)^+}\ |y\right]\right) \leq \mathbb{E}\left[\left(\mathbb{E}[\ |x|\ |\ y]\right)^2\right].$$

Proof: Note that

$$\begin{aligned}&\mathbb{V}ar\left(\mathbb{E}\left[1 - \sqrt{(1+x)^+}\ |y\right]\right)\\ &\quad\leq \mathbb{E}\left[\mathbb{E}\left[1 - \sqrt{(1+x)^+}\ |y\right]^2\right].\end{aligned}$$

Since for any x, $|1 - \sqrt{(1+x)^+}| \leq |x|$,

$$\left|\mathbb{E}\left[1 - \sqrt{(1+x)^+}\ |y\right]\right| \leq \mathbb{E}[\ |x|\ |\ y]$$

is satisfied for any y, which completes the proof. ■

Now, we can proceed with the proof of the theorem. Assume without loss of generality that $\rho_{\min} = \min(\rho_1, \rho_2) = \rho_1$. When $\hat{\boldsymbol{\phi}}_e \neq \emptyset$, we can obtain an upper bound on the secret key rate as follows.

$$\begin{aligned}R_U &= \lim_{n\to\infty} \frac{1}{n} I(\hat{\mathbf{d}}_1; \hat{\mathbf{d}}_2 | \hat{\mathbf{d}}_{1e}, \hat{\mathbf{d}}_{2e}, \hat{\boldsymbol{\phi}}_e)\\ &\leq \lim_{n\to\infty} \frac{1}{n}\big(h(\hat{\mathbf{d}}_1|\hat{\mathbf{d}}_{1e}, \hat{\mathbf{d}}_{2e}, \hat{\boldsymbol{\phi}}_e) - h(\hat{\mathbf{d}}_1|\mathbf{d}_{12})\big) \qquad (36)\\ &\leq \lim_{n\to\infty} \frac{1}{n}\sum_{i=1}^{n}\Big(h(\hat{d}_1[i]|\hat{d}_{1e}[i], \hat{d}_{2e}[i], \hat{\phi}_e[i]) -\\ &\qquad h(\hat{d}_1[i] - d_{12}[i]|d_{12}[i])\Big)\\ &= h(\hat{d}_1|\hat{d}_{1e}, \hat{d}_{1e}, \hat{\phi}_e) - h(\hat{d}_1 - d_{12}|d_{12}) \qquad (37)\end{aligned}$$

where (36) follows from the fact that $\hat{\mathbf{d}}_1 \to \mathbf{d}_{12} \to (\hat{\mathbf{d}}_2, \hat{\mathbf{d}}_{1e}, \hat{\mathbf{d}}_{2e}, \hat{\boldsymbol{\phi}}_e)$ forms a Markov chain, and (37) follows from the fact that all of the random variables $\hat{d}_1[i], \hat{d}_{1e}[i], \hat{d}_{2e}[i], \hat{\phi}_e[i]$ have a stationary distribution, denoted as $\hat{d}_1, \hat{d}_{1e}, \hat{d}_{2e}$ and $\hat{\phi}_e$, respectively. The second term in (37) can be directly found as

$$h(\hat{d}_1 - d_{12}|d_{12}) = \frac{1}{2}\mathbb{E}\left[\log\left(\frac{\gamma(d_{12})\rho_1}{P}\right)\right] \tag{38}$$

from the definition of $\hat{d}_1[i]$. Now, we bound the first term in (37). Let us define

$$\hat{d}_e \triangleq \sqrt{[\hat{d}_{1e}^2 + \hat{d}_{2e}^2 - 2\hat{d}_{1e}\hat{d}_{2e}\cos(\hat{\phi}_e)]^+}.$$

Then,

$$h(\hat{d}_1|\hat{d}_{1e},\hat{d}_{2e},\hat{\phi}_e) \le h\big(\hat{d}_1|\hat{d}_e\big) \le h\big(\hat{d}_1-\hat{d}_e\big). \tag{39}$$

Note that for a given variance, Gaussian distribution maximizes the entropy. Therefore, the entropy of a Gaussian random variable that has a variance identical to that of $\hat{d}_1-\hat{d}_e$ will be an upper bound for (39). We proceed as follows.

$$\mathbb{V}ar\big(\hat{d}_1-\hat{d}_e\big) = \mathbb{E}\big[\mathbb{V}ar\big(\hat{d}_1-\hat{d}_e|d_{12},d_{1e},d_{2e}\big)\big] + \mathbb{V}ar\big(\mathbb{E}\big[\hat{d}_1-\hat{d}_e|d_{12},d_{1e},d_{2e}\big]\big), \tag{40}$$

where (40) follows from the fact that for any dependent random variables x and y, $\mathbb{V}ar(x)=\mathbb{E}[\mathbb{V}ar(x|y)]+\mathbb{V}ar(\mathbb{E}[x|y])$. We now find an upper bound on the first term of (40). Note that,

$$\mathbb{V}ar\big(\hat{d}_1-\hat{d}_e|d_{12},d_{1e},d_{2e}\big) = \mathbb{V}ar\big(\hat{d}_1|d_{12}\big)+\mathbb{V}ar\big(\hat{d}_e|d_{12},d_{1e},d_{2e}\big) \tag{41}$$

due to Lemma 1, since $\hat{d}_1 \to (d_{12},d_{1e},d_{2e}) \to (\hat{d}_{1e},\hat{d}_{2e},\hat{\phi}_e) \to \hat{d}_e$ forms a Markov chain, and the fact that $\hat{d}_1$ is independent of d_{1e},d_{2e} given d_{12}. The first term in (41) is equal to

$$\mathbb{V}ar(\hat{d}_1|d_{12}) = \mathbb{V}ar\big(w_1|d_{12}\big) = \frac{\gamma(d_{12})\rho_1}{P}. \tag{42}$$

We bound the second term in (41) as follows. Let us define κ as

$$\kappa \triangleq \frac{1}{d_{12}^2}\Big(2(d_{1e}-d_{2e}\cos(\hat{\phi}_e))w_{1e}+{w_{1e}}^2 + {w_{2e}}^2+2(d_{2e}-d_{1e}\cos(\hat{\phi}_e))w_{2e} + 2d_{1e}d_{2e}(\cos(\phi_e)-\cos(\hat{\phi}_e)) - 2w_{1e}w_{2e}\cos(\hat{\phi}_e)\Big).$$

Then,

$$\begin{aligned}&\mathbb{V}ar(\hat{d}_e|d_{12},d_{1e},d_{2e})\\ &= \mathbb{V}ar\Big\{\Big(\Big[d_{1e}^2+d_{2e}^2+2(d_{1e}-d_{2e}\cos\hat{\phi}_e)w_{1e}+ 2(d_{2e}-d_{1e}\cos\hat{\phi}_e)w_{2e}-2d_{1e}d_{2e}\cos\hat{\phi}_e+{w_{1e}}^2 + {w_{2e}}^2-2w_{1e}w_{2e}\cos\hat{\phi}_e\Big]^+\Big)^{0.5}|d_{12},d_{1e},d_{2e}\Big\} \quad (43)\\ &\le d_{12}^2\mathbb{V}ar(\sqrt{[1+\kappa]^+}), \quad (44)\end{aligned}$$

where (43) follows due to the definitions of $\hat{d}_{1e}$, $\hat{d}_{2e}$ and $\hat{\phi}_e$. (44) follows due to definition of κ, and the cosine law $d_{12}^2=d_{1e}^2+d_{2e}^2-2d_{1e}d_{2e}\cos(\phi_e)$. Now we will apply Lemma 2 to bound (44). First, note that

$$\begin{aligned}\mathbb{E}[\kappa] &= \frac{1}{d_{12}^2}\mathbb{E}\Big[w_{1e}^2+w_{2e}^2-2d_{1e}d_{2e}(\cos\phi_e-\cos\hat{\phi}_e)\Big]\\ &\ge \frac{1}{Pd_{12}^2}\mathbb{E}\Big[w_{1e}^2+w_{2e}^2-2d_{1e}d_{2e}|w_{\phi_e}|\Big]\\ &\ge \frac{\rho_e}{Pd_{12}^2}\mathbb{E}\Big[\gamma(d_{1e})+\gamma(d_{2e}) - 2d_{1e}d_{2e}\sqrt{\frac{2P\gamma_\phi(d_{1e},d_{2e})}{\pi\rho_e}}\Big], \quad (45)\end{aligned}$$

where (45) follows from the fact that since w_{ϕ_e} is zero mean Gaussian, $|w_{\phi_e}|$ follows a Half-normal distribution with $\mathbb{E}(|w_{\phi_e}|)=\sqrt{\frac{2\gamma_\phi(d_{1e},d_{2e})\rho_e}{P\pi}}$. We can choose P_1 such that for any beacon power $P>P_1$, $\mathbb{E}[x]>-\frac{3}{4}$. Let $\mu=-\frac{3}{4}$, and $\alpha=\frac{\sqrt{1+\mu}}{1+\mu}=2$. Due to Lemma 2, we obtain

$$\begin{aligned}d_{12}^2\mathbb{V}ar(\sqrt{[1+\kappa]^+}) &\le d_{12}^2\mathbb{V}ar(\alpha\kappa)\\ &\le \frac{4\alpha^2}{d_{12}^2}\Big(\mathbb{V}ar(2(d_{1e}-d_{2e}\cos(\hat{\phi}_e))w_{1e}) \quad (46)\\ &\quad+\mathbb{V}ar(2(d_{2e}-d_{1e}\cos(\hat{\phi}_e))w_{2e})\\ &\quad+\mathbb{V}ar(2d_{1e}d_{2e}(\cos(\phi_e)-\cos(\hat{\phi}_e)))\\ &\quad+\mathbb{V}ar(2w_{1e}w_{2e}\cos(\hat{\phi}_e))\\ &\quad+\mathbb{V}ar(w_{1e}^2)+\mathbb{V}ar(w_{2e}^2)\Big)\\ &\le \mathbb{E}\Big[\frac{16\rho_e}{Pd_{12}^2}\Big(4(d_{1e}+d_{2e})^2(\gamma(d_{1e})+\gamma(d_{2e})) \quad (47)\\ &\quad+4(d_{1e}d_{2e})^2\gamma_\phi(d_{1e},d_{2e})+o\left(\frac{1}{P}\right)\Big)\Big], \quad (48)\end{aligned}$$

where (46) follows from applying Lemma 1 to $\mathbb{V}ar(\kappa)$ twice, and (48) follows from the fact that

$$\mathbb{V}ar(2(d_{ie}-d_{je}\cos(\hat{\phi}_e))w_{ie}) \le \mathbb{V}ar(2(d_{ie}+d_{je})w_{ie})$$

for $i,j\in\{1,2\}$, and

$$\begin{aligned}&\mathbb{V}ar(2d_{1e}d_{2e}(\cos(\phi_e)-\cos(\hat{\phi}_e)))\\ &\quad=\mathbb{V}ar(2d_{1e}d_{2e}(\cos(\phi_e)-\cos(\phi_e+w_\phi))\\ &\quad\le\mathbb{V}ar(2d_{1e}d_{2e}w_\phi).\end{aligned}$$

Now, we find an upper bound for the second term of (40) as follows.

$$\begin{aligned}&\mathbb{V}ar\big(\mathbb{E}\big[\hat{d}_1-\hat{d}_e|d_{12},d_{1e},d_{2e}\big]\big)\\ &= \mathbb{V}ar\Big(d_{12}\mathbb{E}\Big[1-\sqrt{(1+\kappa)^+}|d_{12},d_{1e},d_{2e}\Big]\Big) \quad (49)\\ &\le \mathbb{E}\left[d_{12}^2\left(\mathbb{E}\big[|x|\ |d_{12},d_{1e},d_{2e}\big]\right)^2\right] \quad (50)\\ &\le \mathbb{E}\Big[\frac{1}{d_{12}^2}\mathbb{E}\big[2(d_{1e}+d_{2e})(|w_{1e}|+|w_{2e}|)+w_{1e}^2+w_{2e}^2\end{aligned}$$

$$+ 2d_{1e}d_{2e}|w_{\phi_e}| + 2|w_{1e}w_{2e}| \ |d_{12}, d_{1e}, d_{2e}\Big]^2\Bigg]$$
$$= \mathbb{E}\Bigg[\frac{\rho_e^2}{Pd_{12}^2}\Bigg(2(d_{1e}+d_{2e})\frac{\sqrt{\gamma(d_{1e})}+\sqrt{\gamma(d_{2e})}}{\sqrt{\rho_e}}$$
$$+ 2d_{1e}d_{2e}\gamma_\phi(d_{1e},d_{2e})$$
$$+ \frac{\gamma(d_{1e})+\gamma(d_{2e})}{\sqrt{P}} + 2\frac{\sqrt{\gamma(d_{1e})+\gamma(d_{2e})}}{\sqrt{P\rho_e}}\Bigg)^2\Bigg] \quad (51)$$
$$= \mathbb{E}\Bigg[\frac{\rho_e^2}{Pd_{12}^2}\Bigg(\frac{4(d_{1e}+d_{2e})^2}{\rho_e}(\sqrt{\gamma(d_{1e})}+\sqrt{\gamma(d_{2e})})^2$$
$$+ 4(d_{1e}d_{2e}\gamma_\phi(d_{1e},d_{2e}))^2$$
$$+ \frac{8(d_{1e}+d_{2e})d_{1e}d_{2e}}{\rho_e}\big(\sqrt{\gamma(d_{1e})}$$
$$+ \sqrt{\gamma(d_{2e})}\big)\sqrt{\gamma_\phi(d_{1e},d_{2e})}\Bigg)\Bigg] + o(1/P). \quad (52)$$

where (49) follows from the fact that $\hat{d}_e = d_{12}\sqrt{(1+\kappa)^+}$, and (50) follows from Lemma 3. Finally, we obtain

$$R_U \le h(\hat{d}_1 - \hat{d}_e) - h(\hat{d}_1 - d_{12}|d_{12}) \quad (53)$$
$$\le \frac{1}{2}\log\Big(2\pi\mathbb{V}ar(\hat{d}_1-\hat{d}_e)\Big) - h(w_1|d_{12}) \quad (54)$$
$$= \frac{1}{2}\log\Bigg\{2\pi\mathbb{E}\Bigg[\frac{\rho_e}{d_{12}^2P}\Bigg(\frac{d_{12}^2\rho_1}{\rho_e}\gamma(d_{12})$$
$$+ 4(d_{1e}+d_{2e})^2(\sqrt{\gamma(d_{1e})}+\sqrt{\gamma(d_{2e})})^2$$
$$+ (4d_{1e}d_{2e}+64(d_{1e}d_{2e})^2)\gamma_\phi(d_{1e},d_{2e})$$
$$+ 8(d_{1e}+d_{2e})d_{1e}d_{2e}\big(\sqrt{\gamma(d_{1e})}$$
$$+ \sqrt{\gamma(d_{2e})}\big)\sqrt{\gamma_\phi(d_{1e},d_{2e})}$$
$$+ 64(d_{1e}+d_{2e})^2(\gamma(d_{1e})+\gamma(d_{2e}))\Bigg) + o\left(\frac{1}{P}\right)\Bigg]\Bigg\}$$
$$- \frac{1}{2}\mathbb{E}\Bigg[\log\left(\frac{2\pi\rho_1\gamma(d_{12})}{P}\right)\Bigg], \quad (55)$$

where (53) follows from (37) and (39), (54) follows from the fact that entropy of $\hat{d}_1 - \hat{d}_e$ is upper bounded by the entropy of a Gaussian random variable that has the same variance as $\hat{d}_1 - \hat{d}_e$. The first term of (55) is obtained by combining combining (42), (48) and (52), and the second term of (55) follows from (38). Note that as $P \to \infty$, the P terms in (55) cancel each other since for any random variables u and v,

$$\lim_{P\to\infty}\log\mathbb{E}\left[\frac{u}{P}+o\Big(\frac{1}{P}\Big)\right] - \mathbb{E}\left[\log\Big(\frac{v}{P}\Big)\right] = \log\mathbb{E}[u] - \mathbb{E}[\log(v)],$$

hence $\lim_{P\to\infty} R_U < \infty$.

B. Proof of Theorem 3

When the eavesdropper does not observe the angle, $\hat{\boldsymbol{\phi}}_e = \emptyset$. Hence

$$R_L = \lim_{n\to\infty}\frac{1}{n}\Big(h(\hat{\mathbf{d}}_1|\hat{\mathbf{d}}_{1e},\hat{\mathbf{d}}_{2e}) - h(\hat{\mathbf{d}}_1|\hat{\mathbf{d}}_2)\Big) \quad (56)$$

First, we show that the first term in (56) is finite.

$$\lim_{P,n\to\infty}\frac{1}{n}h(\hat{\mathbf{d}}_1|\hat{\mathbf{d}}_{1e},\hat{\mathbf{d}}_{2e}) = \lim_{n\to\infty}\frac{1}{n}h(\mathbf{d}_{12}|\mathbf{d}_{1e},\mathbf{d}_{2e})$$
$$= \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}h(d_{12}[i]|\mathbf{d}_{1e},\mathbf{d}_{2e},\{d_{12}[j]\}_{j=1}^{i-1})$$
$$= \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}h(d_{12}[i]|\mathbf{d}_{1e},\mathbf{d}_{2e},\{\phi_e[j]\}_{j=1}^{i-1}) \quad (57)$$
$$= \lim_{n\to\infty}\frac{1}{n}\sum_{i=1}^{n}h\Bigg(\big(d_{1e}[i]^2+d_{2e}[i]^2-$$
$$2d_{1e}[i]d_{2e}[i]\cos(\phi_e[i])\big)^{0.5}|\mathbf{d}_{1e},\mathbf{d}_{2e},\{\phi_e[j]\}_{j=1}^{i-1}\Bigg) \quad (58)$$
$$> -\infty \quad (59)$$

where (57) follows from the fact that a triangle is completely characterized by either three sides $(d_{12}[i]\, d_{1e}[i], d_{2e}[i])$, or two sides and an angle $(d_{12}[i]\, d_{1e}[i], \phi_e[i])$. Equation (58) follow from the cosine law. Since the probability density function of $\boldsymbol{\phi}_e, \mathbf{d}_{12}$ and $\mathbf{d}_{1e}, \mathbf{d}_{2e}$ are well defined, we can see that $h(\phi_e[i]|\mathbf{d}_{1e},\mathbf{d}_{2e},\{\phi_e[j]\}_{j=1}^{i-1}) > -\infty$, hence (59) holds. The second term

$$\frac{1}{n}h(\hat{\mathbf{d}}_1|\hat{\mathbf{d}}_2) \le \frac{1}{n}h(\hat{\mathbf{d}}_1-\hat{\mathbf{d}}_2) \quad (60)$$
$$= h(w_1-w_2)$$
$$\le \frac{1}{2}\log\left(2\pi\mathbb{E}\left[\frac{4\rho_{\max}\gamma(d_{12})}{P}\right]\right) \quad (61)$$
$$= \frac{1}{2}\log\left(2\pi\mathbb{E}\left[4\rho_{\max}\gamma(d_{12})\right]\right) - \frac{1}{2}\log(P).$$

where (60) follows due to the fact that conditioning reduces entropy, (61) follows from the fact $\hat{d}_1[i]-\hat{d}_2[i] = w_1[i]-w_2[i]$ for any i. Dropping the index i, we can see that $h(w_1-w_2)$ is upper bounded by entropy of a Gaussian random variable that has the same variance as w_1-w_2, which is

$$\mathbb{V}ar(w_1-w_2) = \mathbb{V}ar(\mathbb{E}[w_1-w_2]) + \mathbb{E}(\mathbb{V}ar[w_1-w_2])$$
$$= \mathbb{E}_{d_{12}}(\mathbb{V}ar[w_1-w_2])$$
$$\le \mathbb{E}\left[\frac{4\rho_{\max}\gamma(d_{12})}{P}\right].$$

Therefore, we can see that

$$\lim_{P\to\infty}\frac{R_L}{\frac{1}{2}\log(P)} \ge 1.$$

Now, we find an upper bound on R_U. Note that

$$\begin{aligned} R_U &= \lim_{n\to\infty} \frac{1}{n} I(\hat{\mathbf{d}}_1; \hat{\mathbf{d}}_2 | \hat{\mathbf{d}}_{1e}, \hat{\mathbf{d}}_{2e}) \\ &\leq \lim_{n\to\infty} \frac{1}{n} \big(h(\hat{\mathbf{d}}_1 | \hat{\mathbf{d}}_{1e}, \hat{\mathbf{d}}_{2e}) - h(\hat{\mathbf{d}}_1 | \mathbf{d}_{12}) \qquad (62) \end{aligned}$$

where the first term of (62) is finite. The second term can be upper bounded as

$$\begin{aligned} \frac{1}{n} h(\hat{\mathbf{d}}_1 | \mathbf{d}_{12}) &= h(w_1 | d_{12}) \\ &\geq \mathbb{E}\left[\frac{1}{2} \log\left(\frac{2\pi\rho_1 \gamma(d_{12})}{P} \right) \right] \\ &= \frac{1}{2} \mathbb{E}\left[\log\left(2\pi\rho_1 \gamma(d_{12}) \right) \right] - \frac{1}{2} \log(P), \end{aligned}$$

therefore

$$\lim_{P\to\infty} \frac{R_U}{\frac{1}{2}\log(P)} \leq 1.$$

Since $R_L \leq R_U$ by definition, the proof is complete.

Appendix C
On Observation Bias

Nodes' observations may have bias due to several factors. In this section, we consider two different source of bias; clock mismatch and multipath fading. We will see that different types of bias may have different outcomes. In this part, we present our results for the GLI case. However, the conclusions are valid for perfect GLI case as well.

A. Clock Mismatch

Assume that there is a clock mismatch between nodes 1, and 2. Consequently, all the observations of d_{12} of nodes 1 and 2 in localization phase are shifted by a random value η_1 and η_2 respectively:

$$\hat{d}_j[i] = d_{12}[i] + w_j[i] + \eta_j \qquad (63)$$

for $j \in \{1, 2\}$, where $w_j[i]$ is as given in (1). We assume the amount of clock mismatch is a non-random, but unknown parameter, which remains constant througout the entire session[8]. Since $w_j[i]$, $j \in \{1, 2\}$ are zero mean random variables,

$$\mathbb{E}[\hat{d}_j[i] | \eta_1, \eta_2] = \mathbb{E}[d_{12}[i]] + \eta_j. \qquad (64)$$

Hence, with the knowledge of the statistics of the mobility, each node $j \in \{1, 2\}$ can obtain a perfect estimate of the amount of clock mismatch η_j as $n \to \infty$, by simply calculating the difference between the long-term average of the distance observations $\hat{d}_j[i]$ for all i and the known mean distance $\mathbb{E}[d_{12}]$. Then this value can be broadcast in the public discussion phase. Therefore, clock mismatch does not affect the theoretical bounds of secret key generation rates.

[8]The underlying assumption is that, the clock mismatch variations are much slower than the duration of the key-generation sessions

B. Multipath Fading

There may be a bias in the observations when the nodes experience multipath fading. An example of this is time of arrival observation of distances when the nodes are not within their line of sight. Note that, this kind of bias does not remain constant, and varies from one slot to the other. The impact of fading can be viewed as that of an additional observation noise source and the distance observations can be written as

$$\hat{d}_j[i] = d_{12}[i] + w_j[i] + \eta_j[i]$$

for $j \in \{1, 2\}$.

Consequently, one will observe a reduction in the key rate. For example, with no angle observation at the eavesdropper, we know from Section V-B that the key rate grows unboundedly with the beacon power P. However, with multipath fading, independent over different locations,

$$\begin{aligned} \lim_{P\to\infty} h(\hat{\mathbf{d}}_1 | \hat{\mathbf{d}}_2) &= h(\boldsymbol{\eta}_1 | \boldsymbol{\eta}_2) \\ &\overset{(a)}{=} h(\boldsymbol{\eta}_1) > -\infty, \end{aligned}$$

where $\boldsymbol{\eta}_1 = \{\eta_1[i]\}_{i=1}^n$, and (a) follows since $\boldsymbol{\eta}_1$ and $\boldsymbol{\eta}_2$ are independent. Hence, following an identical approach to Section V-B, one see that $\lim_{P\to\infty} R_L < \infty$, i.e., the secret key rate remains bounded even as the power grows unboundedly.

References

[1] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Information Theory*, vol.39, no.3, pp.733-742, May 1993

[2] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Information Theory* , vol.39, no.4, pp.1121-1132, Jul 1993

[3] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Trans. Information Theory* , vol.45, no.2, pp.499-514, Mar 1999

[4] I. Csiszar and P. Narayan, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Information Theory*, vol.54, no.6, pp.2437-2452, June 2008

[5] U. M. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels .I. Definitions and a completeness result," *IEEE Transactions on Information Theory*, vol.49, no.4, pp. 822- 831, April 2003

[6] I. Csiszar and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Transactions on Information Theory*, vol.46, no.2, pp.344-366, Mar 2000

[7] S. Gezici, Z. Tian, G. B. Giannakis, H. Kobayashi, A.F. Molisch, H.V. Poor, and Z. Sahinoglu, "Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks," *IEEE Signal Processing Magazine*, vol.22, no.4, pp. 70- 84, July 2005

[8] Y. Shen and M.Z. Win,"Fundamental limits of wideband localization Part I: A general framework," *IEEE Trans. Information Theory*, vol.56, no.10, pp.4956-4980, Oct. 2010

[9] Y. Shen, H. Wymeersch and M.Z. Win, "Fundamental limits of wideband localization Part II: Cooperative networks," *IEEE Trans. Information Theory*, vol.56, no.10, pp.4981-5000, Oct. 2010

[10] H. Buhrman, N. Chandran, V. Goyal, R. Ostrovsky and C. Schaffner, "Position-based quantum cryptography: Impossibility and constructions,", 2010

[11] A. Srivinasan and J. Vu, "A survey on secure localization in wireless sensor networks", *Encyclopedia of Wireless and Mobile Communications*, 2007

[12] R. Poovendran, C. Wang, S. Roy, "Secure localization and time synchronization for wireless sensor and ad-hoc networks", Springer Verlag, 2007

[13] N. Chandran, V. Goyal, R. Moriarty and R. Ostrovsky, "Position based cryptography," *Cryptology ePrint Archive*, 2009, http://eprint.iacr.org/2009/

[14] Wilson, R.; Tse, D.; Scholtz, R.A.; , "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE International Conf. Ultra-Wideband, ICUWB 2007*, pp.270-275, 24-26 Sept. 2007

[15] S. Verdu and T. S. Han, "A general formula for channel capacity," *IEEE Transactions on Information Theory*, vol.40, no.4, pp.1147-1157, Jul 1994

[16] M. R. Bloch and J. N. Laneman, "Secrecy from resolvability," *arXiv:1105.5419v1 [cs.IT]*, May 2011

[17] P. K. Gopala, L. Lai, and H. El-Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol.54, no.10, pp.4687-4698, October 2008

[18] D. Jourdan, D. Dardari and M. Win, "Position error bound for UWB localization in dense cluttered environments," *IEEE Transactions on Aerospace and Electronic Systems*, vol.44, no.2, pp.613-628, April 2008

[19] T.M. Cover and J.A. Thomas, "Elements of information theory," Wiley, New-York, 2nd edition, 2006

[20] L. R. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," *Proceedings of the IEEE*, vol.77, no.2, pp.257-286, Feb 1989

[21] S. Mathur, W. Trappe, N. Mandayam, C. Ye and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," *Proceedings of the 14th ACM international conference on Mobile computing and networking (MobiCom '08) ACM*, New York, NY, USA, 128-139

[22] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," *Proceedings of the 15th annual international conference on Mobile computing and networking (MobiCom '09) ACM*, New York, NY, USA, 321-332

[23] J. Zhang, S.K. Kasera and N. Patwari, "Mobility Assisted Secret Key Generation Using Wireless Link Signatures," *Proc. IEEE INFOCOM 2010*, vol., no., pp.1-5, 14-19 March 2010

[24] N. Patwari, J. Croft, S. Jana and S. K. Kasera, "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements," *IEEE Transactions on Mobile Computing* , vol.9, no.1, pp.17-30, Jan. 2010

[25] NIST, "A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications," 2001

[26] NIST Computer Security Division, "Secure Hashing", http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html, NIST

[27] G.Brassard and L. Salvail, "Secret-key reconciliation by public discussion," *in Workshop on the theory and application of cryptographic techniques on Advances in cryptology (EUROCRYPT '93)*, Tor Helleseth (Ed.). Springer-Verlag New York, Inc., Secaucus, NJ, USA, 410-423.

[28] C.H. Bennett, G. Brassard, C. Crepeau and U.M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol.41, no.6, pp.1915-1923, Nov 1995